Vectorial bent functions in odd characteristic and their components

Ayça Çeşmelioğlu, Wilfried Meidl, Alexander Pott

Boolean Functions and their Applications 2019, Florence, Italy
Dedicated to the 70th birthday of Claude Carlet

June 18, 2019

Bent functions

p prime, $\mathbb{V}_n$ n-dimensional vector space over $\mathbb{F}_p$, (e.g. $\mathbb{F}_p^n$,$\mathbb{F}_{p^n}$).
A p-ary or Boolean function $f : \mathbb{V}_n \to \mathbb{F}_p$ is called bent if the Walsh transform satisfies

$$|\widehat{f}(b)| = |\sum_{x \in \mathbb{V}_n} \epsilon_p^{f(x)-\langle b,x\rangle}| = p^{n/2},$$

for all $b \in \mathbb{V}_n$ where $\epsilon_p = e^{2\pi i/p}$ and $\langle b, x\rangle$ denotes a (nondegenerate) inner product of $\mathbb{V}_n$.

(Weakly) regular bent functions

Let $f : \mathbb{V}_n \to \mathbb{F}_p$ be a bent function.

If $p = 2$, then $\widehat{f}(b) = (-1)^{f^*(b)} 2^{n/2}$.

If p is odd, then

$$\widehat{f}(b) = \begin{cases} \pm \epsilon_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 1 \bmod 4; \\ \pm i \epsilon_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 3 \bmod 4, \end{cases}$$

$f^* : \mathbb{V}_n \to \mathbb{F}_p$, dual function of the bent function f.

(Weakly) regular bent functions

Let $f : \mathbb{V}_n \to \mathbb{F}_p$ be a bent function.

If $p = 2$, then $\widehat{f}(b) = (-1)^{f^*(b)} 2^{n/2}$.

If p is odd, then

$$\widehat{f}(b) = \begin{cases} \pm \epsilon_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 1 \bmod 4; \\ \pm i \epsilon_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 3 \bmod 4, \end{cases}$$

$f^* : \mathbb{V}_n \to \mathbb{F}_p$, dual function of the bent function f.

f regular bent: $\widehat{f}(b) = \epsilon_p^{f^*(b)} p^{n/2}$

f weakly regular bent: $\widehat{f}(b) = \zeta \epsilon_p^{f^*(b)} p^{n/2}$, $\zeta \in \{\pm 1, \pm i\}$ independent from b

f non-weakly regular bent: "Sign" changes with b

Dual-bent functions

Well known: The dual of a weakly regular bent function is a bent function (again weakly regular)

Dual-bent functions

Well known: The dual of a weakly regular bent function is a bent function (again weakly regular)

But: The dual of a non-weakly regular bent function can be

- a bent function,
- not a bent function.

Dual-bent functions

Well known: The dual of a weakly regular bent function is a bent function (again weakly regular)

But: The dual of a non-weakly regular bent function can be

- a bent function,
- not a bent function.

Definition

(Çeşmelioğlu, M., Pott, 2013) A bent function f is called a dual-bent function if the dual function f^* is also a bent function. Otherwise we call f a non-dual-bent function.

Non weakly regular dual-bent

The "classical" bent functions are (weakly) regular:
Maiorana-McFarland, Spread, Coulter-Matthews, Quadratic bent functions, Helleseth's et al. monomials and binomials, ...

Non weakly regular dual-bent

The "classical" bent functions are (weakly) regular:
Maiorana-McFarland, Spread, Coulter-Matthews, Quadratic bent functions, Helleseth's et al. monomials and binomials, ...

Helleseth et al., 2006, 2010, 2011:

First examples of non-weakly regular bent functions:

Çeşmelioğlu,McGuire, M., J. Combin. Theory B, 2012:

First construction of non-weakly regular bent functions. The functions belong to the class of dual-bent functions.

Non weakly regular dual-bent

The "classical" bent functions are (weakly) regular:
Maiorana-McFarland, Spread, Coulter-Matthews, Quadratic bent functions, Helleseth's et al. monomials and binomials, ...

Helleseth et al., 2006, 2010, 2011:

First examples of non-weakly regular bent functions:

Çeşmelioğlu,McGuire, M., J. Combin. Theory B, 2012:

First construction of non-weakly regular bent functions. The functions belong to the class of dual-bent functions.

Çeşmelioğlu, M., Pott, IEEE Trans. Inform Theory 2016:

First construction of non-dual-bent functions for every odd p.

Vectorial bent functions

Let V_n, V_m be vector spaces over $\mathbb{F}_p$ of dimension n and m, and $\langle , \rangle$ an inner product in V_m. For a vectorial function $F : V_n \to V_m$ and $\alpha \in V_m$, $f_\alpha : V_n \to \mathbb{F}_p$

$$f_\alpha(x) = \langle \alpha, F(x) \rangle$$

is called a component function of F.

Vectorial bent functions

Let V_n, V_m be vector spaces over $\mathbb{F}_p$ of dimension n and m, and $\langle , \rangle$ an inner product in V_m. For a vectorial function $F : V_n \to V_m$ and $\alpha \in V_m$, $f_\alpha : V_n \to \mathbb{F}_p$

$$f_\alpha(x) = \langle \alpha, F(x) \rangle$$

is called a component function of F.

Vectorial bent function $F : V_n \to V_m$: Every (non-zero) component function is bent. (Recall: $m \leq n$ and when $p = 2$ then $m \leq n/2$.)

Observation: The "classical" constructions, Maiorana-McFarland, Spread, Dillon's H-class ($p = 2$), are vectorial constructions.

More examples, $p = 2$

C. Carlet et. al. (IEEE Trans. Inform Theory 64, 2018).

More examples, $p = 2$

C. Carlet et. al. (IEEE Trans. Inform Theory 64, 2018).

I particularly like:
Vectorial Kasami bent function, C. Carlet (Des Codes Cryptogr. 59, 2011):

$$F(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\beta x^{2^{2i}-2^i+1}), n = 2m, m \text{ odd}, \beta \in \mathbb{F}_{2^n} \text{ non-cube.}$$

More examples, $p = 2$

C. Carlet et. al. (IEEE Trans. Inform Theory 64, 2018).

I particularly like:
Vectorial Kasami bent function, C. Carlet (Des Codes Cryptogr. 59, 2011):

$$F(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\beta x^{2^{2i}-2^i+1}), n = 2m, m \text{ odd}, \beta \in \mathbb{F}_{2^n} \text{ non-cube.}$$

It shows that a non-weakly normal bent function can be a component of a vectorial bent function.

Questions

- Find a lonely Boolean bent function

Questions

- Find a lonely Boolean bent function

  Or: Is every Boolean bent function a component function of a vectorial bent function (of dimension at least 2)?

  i.e. is every Boolean bent function the sum of two bent function?

Remark: Tokareva's hypothesis: Every Boolean function in an even number of variables n and of degree at most $n/2$ is the sum of two bent functions.

Questions, p odd

- Is every p-ary bent function, p odd, a component function of a vectorial bent function (of dimension at least 2)?

  i.e. For every p-ary bent function f, does there exist a bent function g such that every nontrivial linear combination $af(x) + bg(x)$ is bent.

Questions, p odd

- Is every p-ary bent function, p odd, a component function of a vectorial bent function (of dimension at least 2)?

  i.e. For every p-ary bent function f, does there exist a bent function g such that every nontrivial linear combination $af(x) + bg(x)$ is bent.

  Or: Find a lonely p-ary bent function.

Questions, p odd

- Is every p-ary bent function, p odd, a component function of a vectorial bent function (of dimension at least 2)?

  i.e. For every p-ary bent function f, does there exist a bent function g such that every nontrivial linear combination $af(x) + bg(x)$ is bent.

  Or: Find a lonely p-ary bent function.

- Can a non-weakly regular bent function be a component of a vectorial bent function?

  Can a non-dual bent function be a component of a vectorial bent function?

Some known classes (weakly regular)

Vectorial constructions: Maiorana-McFarland, p-ary partial spread (on a complete spread), Coulter-Matthews, every quadratic bent function

Some known classes (weakly regular)

Vectorial constructions: Maiorana-McFarland, p-ary partial spread (on a complete spread), Coulter-Matthews, every quadratic bent function

Further classes, Helleseth et al. (2006, 2009, 2010):

(i) $f_1 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_1(x) = \mathrm{Tr}_n\left(ax^{r(3^m-1)}\right)$, $n = 2m$, $\gcd(r, 3^m + 1) = 1$
(with the condition that the Kloosterman sum $K(a) = \sum_{z \in \mathbb{F}_{3^n}} \epsilon_3^{z+a^{3^m+1}/z}$, where $1/0 := 0$, vanishes)

Some known classes (weakly regular)

Vectorial constructions: Maiorana-McFarland, p-ary partial spread (on a complete spread), Coulter-Matthews, every quadratic bent function

Further classes, Helleseth et al. (2006, 2009, 2010):

(i) $f_1 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_1(x) = \mathrm{Tr}_n\left(ax^{r(3^m-1)}\right)$, $n = 2m$, $\gcd(r, 3^m + 1) = 1$
(with the condition that the Kloosterman sum $K(a) = \sum_{z \in \mathbb{F}_{3^n}} \epsilon_3^{z + a^{3^m+1}/z}$, where $1/0 := 0$, vanishes)

Observation: f_1 is a univariate representation of a PS_{ap} bent function, hence a component of a vectorial PS_{ap} bent function.

Some known classes (weakly regular)

Vectorial constructions: Maiorana-McFarland, p-ary partial spread (on a complete spread), Coulter-Matthews, every quadratic bent function

Further classes, Helleseth et al. (2006, 2009, 2010):

(i) $f_1 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_1(x) = \mathrm{Tr}_n\left(ax^{r(3^m-1)}\right)$, $n = 2m$, $\gcd(r, 3^m + 1) = 1$
(with the condition that the Kloosterman sum $K(a) = \sum_{z \in \mathbb{F}_{3^n}} \epsilon_3^{z + a^{3^m+1}/z}$, where $1/0 := 0$, vanishes)

Observation: f_1 is a univariate representation of a PS_{ap} bent function, hence a component of a vectorial PS_{ap} bent function.

(ii) $f_2 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_2(x) = \mathrm{Tr}_n\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)$, $n = 4k$.

Some known classes (weakly regular)

Vectorial constructions: Maiorana-McFarland, p-ary partial spread (on a complete spread), Coulter-Matthews, every quadratic bent function

Further classes, Helleseth et al. (2006, 2009, 2010):

(i) $f_1 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_1(x) = \mathrm{Tr}_n\left(ax^{r(3^m-1)}\right)$, $n = 2m$, $\gcd(r, 3^m + 1) = 1$
(with the condition that the Kloosterman sum $K(a) = \sum_{z\in\mathbb{F}_{3^n}} \epsilon_3^{z+a^{3^m+1}/z}$, where $1/0 := 0$, vanishes)

Observation: f_1 is a univariate representation of a PS_{ap} bent function, hence a component of a vectorial PS_{ap} bent function.

(ii) $f_2 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_2(x) = \mathrm{Tr}_n\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)$, $n = 4k$.

Observation: f_2 is component of the vectorial bent function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$,

$$F(x) = \mathrm{Tr}_k^{4k}(x^{p^{3k}+p^{2k}-p^k+1} + x^2).$$

Some known classes (weakly regular)

(iii) $f_3 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_3(x) = \mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)$, $n = 2m$, m odd, $a = \alpha^{(3^m+1)/4}$ for a primitive element α of $\mathbb{F}_{3^n}$;

Some known classes (weakly regular)

(iii) $f_3 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_3(x) = \mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)$, $n = 2m$, m odd, $a = \alpha^{(3^m+1)/4}$ for a primitive element α of $\mathbb{F}_{3^n}$;

Result: f_3 is a component of the vectorial bent function $F : \mathbb{F}_{3^n} \to \mathbb{F}_{3^m}$,

$$F(x) = \mathrm{Tr}_m^n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right).$$

Some known classes (weakly regular)

(iii) $f_3 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_3(x) = \mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)$, $n = 2m$, m odd,
$a = \alpha^{(3^m+1)/4}$ for a primitive element α of $\mathbb{F}_{3^n}$;

Result: f_3 is a component of the vectorial bent function
$F : \mathbb{F}_{3^n} \to \mathbb{F}_{3^m}$,

$$F(x) = \mathrm{Tr}_m^n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right).$$

We use p-ary version of Carlet et al, 2018, Lemma 1, Proposition 1
(Let $f(x) = \mathrm{Tr}_n(ax^d)$ be a monomial bent function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with d satisfying

$$\gcd\left(\frac{d}{\gcd(d,t)}, p^m - 1\right) = 1,\ t = (p^n-1)/(p^m-1)$$

for some divisor m of n. Then the function $F(x) = \mathrm{Tr}_m^n(ax^d)$ is a vectorial bent function.)

Non-weakly regular, non-dual components

Non-weakly regular, non-dual components

The semi-direct sum Çeşmelioğlu, M., Pott, 2016:

Let $f : V_m \to \mathbb{F}_p$ and $g : V_n \to \mathbb{F}_p$ be bent, and let h be a function from V_m to V_n. Define $F : V_m \times V_n \to \mathbb{F}_p$ as

$$F(x, y) = f(x) + g(y + h(x)).$$

Non-weakly regular, non-dual components

The semi-direct sum Çeşmelioğlu, M., Pott, 2016:

Let $f : V_m \to \mathbb{F}_p$ and $g : V_n \to \mathbb{F}_p$ be bent, and let h be a function from V_m to V_n. Define $F : V_m \times V_n \to \mathbb{F}_p$ as

$$F(x, y) = f(x) + g(y + h(x)).$$

$F(x, y)$ is bent if and only if for all $b \in V_n$ the function $G_b : V_m \to \mathbb{F}_p$

$$G_b(x) = f(x) + \langle b, h(x) \rangle$$

is a bent function. The dual F^* of F is then

$$F^*(x, y) = G_y^*(x) + g^*(y).$$

The semi-direct sum

$f : V_m \to \mathbb{F}_p$ and $g : V_n \to \mathbb{F}_p$ bent, $h : V_m \to V_n$.

$$F(x, y) = f(x) + g(y + h(x))$$

Remark 1: If $h = 0$ then the semi-direct sum reduces to the direct sum $f(x) + g(y)$

The semi-direct sum

$f : V_m \to \mathbb{F}_p$ and $g : V_n \to \mathbb{F}_p$ bent, $h : V_m \to V_n$.

$$F(x, y) = f(x) + g(y + h(x))$$

Remark 1: If $h = 0$ then the semi-direct sum reduces to the direct sum $f(x) + g(y)$

Remark 2: If $p = 2$ and $g(y) = y_1 y_2 + y_3 y_4 + \cdots + y_{n-1} y_n$, then F is of the form

$$F(x, y_1, \ldots, y_n) = f(x) + \sum_{i=1}^{n/2} (y_{2i-1} + h_{2i-1}(x))(y_{2i} + h_{2i}(x)).$$

(Secondary bent function construction, C. Carlet 1991)

The semi-direct sum of bent functions, Version 2

Çeşmelioğlu, M., Pott, 2019: Let $f : \mathbb{V}_m \to \mathbb{F}_{p^k}$ and $g : \mathbb{V}_n \to \mathbb{F}_{p^k}$ be vectorial bent functions, h be a function from $\mathbb{V}_m$ to $\mathbb{V}_n$. Then $F : \mathbb{V}_m \times \mathbb{V}_n \to \mathbb{F}_{p^k}$

$$F(x, y) = f(x) + g(y + h(x))$$

is vectorial bent if and only if for all $b \in \mathbb{V}_n$ and nonzero $\alpha \in \mathbb{F}_{p^k}$ the p-ary function

$$G_{b,\alpha}(x) = \mathrm{Tr}_k(\alpha f(x)) + \langle b, h(x) \rangle_n$$

is bent.

Non-dual bent functions and vectorial bent functions

Choose $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$, $f(x) = \mathrm{Tr}_k^m(x^2)$ and $g : \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, $g(y_1, y_2) = y_1 y_2$.

Non-dual bent functions and vectorial bent functions

Choose $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$, $f(x) = \mathrm{Tr}_k^m(x^2)$ and
$g : \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, $g(y_1, y_2) = y_1 y_2$.

Theorem

Let $m = 3k$, and let $\{1, \gamma_1, \gamma_2\}$ be a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^k}$. Then
$F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$,

$$F(x, y_1, y_2) = \mathrm{Tr}_k^m(x^2) + (y_1 + \mathrm{Tr}_k^m(\gamma_1 x^2))(y_2 + \mathrm{Tr}_k^m(\gamma_2 x^2))$$

is a vectorial bent function.

Non-dual bent functions and vectorial bent functions

Choose $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$, $f(x) = \mathrm{Tr}_k^m(x^2)$ and
$g : \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, $g(y_1, y_2) = y_1 y_2$.

Theorem

Let $m = 3k$, and let $\{1, \gamma_1, \gamma_2\}$ be a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^k}$. Then
$F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$,

$$F(x, y_1, y_2) = \mathrm{Tr}_k^m(x^2) + (y_1 + \mathrm{Tr}_k^m(\gamma_1 x^2))(y_2 + \mathrm{Tr}_k^m(\gamma_2 x^2))$$

is a vectorial bent function.
Dual of the component function $F_\alpha(x, y_1, y_2) = \mathrm{Tr}_k(\alpha F(x, y_1, y_2))$:

$$F_\alpha^*(x, y_1, y_2) = -\mathrm{Tr}_m\left(\frac{x^2}{4(\alpha + y_1\gamma_1 + y_2\gamma_2)}\right) - \mathrm{Tr}_k(y_1 y_2/\alpha).$$

Non-dual bent functions and vectorial bent functions

Corollary

Let η be the quadratic character in $\mathbb{F}_{p^k}$. If for some nonzero $\alpha \in \mathbb{F}_{p^k}$ we have

$$\Big| \sum_{y_1, y_2 \in \mathbb{F}_{p^k}} \eta(\alpha + y_1\gamma_1 + y_2\gamma_2)\epsilon_p^{-\mathrm{Tr}_k(y_1y_2/\alpha)} \Big| \neq p^k,$$

then F^*_α is not bent. Consequently F is a vectorial bent function which has non-dual-bent component functions.

($\{1, \gamma_1, \gamma_2\}$ basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^k}$)

THANK YOU