On bentness, the nonlinearity and bent components of vectorial functions

Sihem Mesnager, University of Paris VIII-LAGA
(joint work with Claude Carlet, Chuankun Wu and Yuwei Xu)

BFA 2018
Loen, Norway, June 2018

Table of contents

Finite fields

$\mathbb{F}_{2^n}$: finite field of order 2^n (characteristic two), n integer

Absolute trace : $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$, $x \in \mathbb{F}_{2^n}$

Trace : $Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^i}$, $m|n$, $x \in \mathbb{F}_{2^n}$

Transitivity property : $Tr_k^m \circ Tr_m^n = Tr_k^n$, $k|m$, $m|n$
$(\mathbb{F}_{2^k} \subset \mathbb{F}_{2^m} \subset \mathbb{F}_{2^n})$

Vectorial functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, n, m two integers

Component function : $Tr_1^m(uF)$, $u \in \mathbb{F}_{2^m}^{\star}$

Monomial vectorial function : $Tr_m^n(ax^d)$, $m|n$, $a \in \mathbb{F}_{2^n}^{\star}$, d integer

Monomial Boolean function : $Tr_1^n(ax^d)$, $a \in \mathbb{F}_{2^n}^{\star}$, d integer

Walsh transform

n, m positive integers

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Extended Walsh transform : $W_F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^n} \to \mathbb{Z}$,

$$W_F(u,v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(uF(x)) + Tr_1^n(vx)}, (u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$$

$W_F(u,v)$: Walsh transform of the Boolean function $Tr_1^n(uF)$ at v.

EA-equivalence

Definition

Two vectorial functions F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ are EA-equivalent if and only if $F' = A \circ F \circ A' + A''$ for some $A \in AGL(\mathbb{F}_{2^n})$, $A' \in AGL(\mathbb{F}_{2^m})$ and A'' is an affine function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$

Extended Walsh spectrum : $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$,

$$\mathcal{W}_F = \{W_F(u,v), (u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}\}$$

Proposition

Let F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ being EA-equivalent. Then, $\mathcal{W}_F = \mathcal{W}_{F'}$.

CCZ-equivalence (Carlet-Charpin-Zinoviev-equivalence)

Definition

The graph of a vectorial function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is $\{(x, F(x)), x \in \mathbb{F}_{2^n}\}$.

Definition

Two vectorial functions F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ are CCZ-equivalent if and only if $G_{F'} = \mathcal{L}(G_F)$ for some affine automorphism $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$.

Proposition

Let F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ being CCZ-equivalent. Then, they are EA-equivalent. Furthermore, they have the same extended Walsh spectrum.

Nonlinearity of S-Boxes

n, m positive integers

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Definition

The nonlinearity of F is

$$\begin{aligned} nl(F) &= \min_{u\in\mathbb{F}_{2^m}} \left(2^{n-1} - \frac{1}{2} \max_{v\in\mathbb{F}_{2^m}^{\star}} |W_F(u,v)|\right) \\ &= 2^{n-1} - \frac{1}{2} \max_{v\in\mathbb{F}_{2^m}^{\star};\ u\in\mathbb{F}_{2^n}} |W_F(u,v)| \end{aligned}$$

Fact

Let F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ being CCZ-equivalent. Then, $nl(F') = nl(F)$.

Bent vectorial functions

n, m positive integers

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Covering radius bound :

$$nl(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

Definition

A vectorial function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is said to be *bent* if $nl(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

Theorem (Nyberg, 1994)

Bent vectorial functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ exist only if n is even and $m \leq \frac{n}{2}$

Theorem (Budaghyan and Carlet, 2011)

CCZ-equivalence and EA-equivalence coincide for bent vectorial functions.

Maiorana-MacFarland Class

$n = 2k$, m positive integer

Maiorana MacFarland Class :

$\mathbb{F}_{2^n} \simeq \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$

$$F(x, y) = L(x\pi(y)) + H(y), \quad (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$$

with :

- $L : \mathbb{F}_{2^k} \to \mathbb{F}_{2^m}$, linear
- $\pi : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, permutation
- $H : \mathbb{F}_{2^k} \to \mathbb{F}_{2^m}$

Fact

F is bent

Monomial vectorial functions

n, m positive integers, n even, $m|n$, $m \leq \frac{n}{2}$

Monomial vectorial function : $Tr_m^n(ax^d)$

Remark

Since $Tr_{m'}^n(ax^d) = Tr_{m'}^n\left(Tr_m^n(ax^d)\right)$, $Tr_{m'}^n(ax^d)$ is bent for any divisor m' of m if $Tr_m^n(ax^d)$ is bent.

Conversely, if $Tr_m^n(ax^d)$ is not bent, then $Tr_{m'}^n(ax^d)$ cannot be bent for any multiple m' of m

Monomial vectorial functions

Transitivity rule of the trace: $Tr_1^m \circ Tr_m^n = Tr_1^n$

Remark

The components of a monomial vectorial function $Tr_m^n(ax^d)$ are the Boolean functions $Tr_1^n(aux^d)$ with $u \in \mathbb{F}_{2^m}^\star$ since, for every $u \in \mathbb{F}_{2^m}$,

$$Tr_1^m(u Tr_m^n(ax^d)) = Tr_1^m(Tr_m^n(aux^d)) = Tr_1^n(aux^d)$$

Monomial vectorial functions

$n = 2k$, k positive integer

List of integers d for which there exists $a \in \mathbb{F}_{2^n}$ such that $Tr_1^n(ax^d)$ is bent :

Type	Exponent	Condition
PS_{ap}	$a(2^k - 1)$	$\gcd(a, 2^k + 1) = 1$
Kasami	$2^{2s} - 2^s + 1$	$\gcd(s, n) = 1$
Maiorana-McFarland	$2^s + 1$	$n = \gcd(s, n)t$, t even
	$(2^s + 1)^2$	$n = 4r$
	$2^{2s} + 2^s + 1$	$n = 6r$

Monomial vectorial functions

$$\mathcal{B}_d = \{a \in \mathbb{F}_{2^n} \mid Tr_1^n(ax^d) \text{ is bent}\}$$

Proposition

$Tr_m^n(ax^d)$ is bent if and only if $\mathcal{B}_d \supset a\mathbb{F}_{2^m}^\star$

Problem : Given an exponent d in the preceding list, find all cosets $a\mathbb{F}_{2^m}^\star$ which are contained in $\mathcal{B}_d$

Bent monomial vectorial functions

Proposition (Pasalic–Zhang, 2012)

If $Tr_1^n(ax^d)$ is a bent Boolean function and x^d permutes $\mathbb{F}_{2^m}^{\star}$ then $Tr_m^n(ax^d)$ is bent.

The permutation condition on x^d is a necessary condition when $m = \frac{n}{2}$:

Proposition

Let d be a positive integer and n be an even positive integer. Let $m = \frac{n}{2}$. Suppose that $Tr_m^n(ax^d)$ is bent. Then $\gcd(2^m - 1, d) = 1$, that is, x^d is a permutation of $\mathbb{F}_{2^m}$.

Theorem

Let $m = \frac{n}{2}$. $Tr_m^n(ax^d)$ is a bent vectorial function if and only if $Tr_1^n(ax^d)$ is a bent Boolean function and x^d permutes $\mathbb{F}_{2^m}^{\star}$.

Gold Case : $d = 2^s + 1$, $\frac{n}{\gcd(s,n)}$ even

Theorem

$\mathcal{B}_d = \mathbb{F}_{2^n} \setminus \{x^{2^s+1}, x \in \mathbb{F}_{2^n}\}$

α primitive element of $\mathbb{F}_{2^n}$

$< \beta > = \{\beta^i, 0 \leq i \leq 2^n - 1\}$, $\beta \in \mathbb{F}_{2^n}^\star$

Lemma

Let e be a positive integer. $a\mathbb{F}_{2^m}^\star \subset \mathbb{F}_{2^n} \setminus \{x^e, x \in \mathbb{F}_{2^n}^\star\}$ *if and only if* $a \notin < \alpha^{\gcd(e,t)} >$ *where* $t = \frac{2^n-1}{2^m-1}$.

Theorem

Let m be a divisor of n. Then, $Tr_m^n(ax^{2^s+1})$ *is bent if and only if* $\gcd(2^s+1, t) \neq 1$ *and* $a \in \mathbb{F}_{2^n}^\star \setminus < \alpha^{\gcd(2^s+1,t)} >$.

Gold Case : $d = 2^s + 1$, $\frac{n}{\gcd(s,n)}$ even

Example

$Tr_4^{12}(ax^9)$ is a bent vectorial function from $\mathbb{F}_{2^{12}}$ to $\mathbb{F}_{2^4}$ provided that a is not a cube of an element of $\mathbb{F}_{2^{12}}$ but x^9 does not permute $\mathbb{F}_{2^4}$ since $\gcd(2^4 - 1, 9) = 3$.

Example

$Tr_3^{12}(ax^9)$ is a bent vectorial function from $\mathbb{F}_{2^{12}}$ to $\mathbb{F}_{2^3}$ provided that a is not a 9th-power of an element of $\mathbb{F}_{2^{12}}$ and x^9 permutes $\mathbb{F}_{2^3}$ since $\gcd(2^3 - 1, 9) = 1$.

Kasami Case : $d = 2^{2s} - 2^s + 1$, $\gcd(s, n) = 1$

Theorem (Dillon - Dobbertin, 2004)

$\mathcal{B}_d = \mathbb{F}_{2^n} \setminus \{x^3, x \in \mathbb{F}_{2^n}\}$

Theorem

Let m be a divisor of n. Then,

- *If m is odd or, if m is even, $\frac{n}{m}$ is a multiple of 3, $Tr_m^n(ax^d)$ is bent if and only if $a \notin < \alpha^3 >$.*
- *If m is even and $\frac{n}{m}$ is not divisible by 3, no vectorial function $Tr_m^n(ax^d)$ is bent.*

Kasami Case : $d = 2^{2s} - 2^s + 1$, $\gcd(s, n) = 1$

Remark

3 is a divisor of $d = 2^{2s} - 2^s + 1$ when $\gcd(s, n) = 1$. If m is odd, 3 and $2^m - 1$ are coprime. Thus, if m is odd, x^d is a permutation of $\mathbb{F}_{2^m}$.

Remark

$Tr_4^{12}(ax^{993})$ is bent provided that a is not a cube of $\mathbb{F}_{2^{12}}$ and x^{993} is not a permutation of $\mathbb{F}_{2^4}$ since $\gcd(2^4 - 1, 993) = 3$.

Leander Case : $d = (2^{\frac{n}{4}} + 1)^2$, $n = 4 \mod 8$

$$A \cdot B = \{ab,\, a \in A,\, b \in B\}$$

Theorem (Leander, 2006, Charpin - Kyureghyan, 2008)

$$\mathcal{B}_d = (\mathbb{F}_4 \setminus \mathbb{F}_2) \cdot \mathbb{F}^{\star}_{2^{\frac{n}{4}}} \cdot \{x^d,\, x \in \mathbb{F}^{\star}_{2^n}\}$$

Theorem

Let m be a divisor of n. Then, $Tr^n_m(ax^d)$ is bent if and only if m is odd and $a \in (\mathbb{F}_4 \setminus \mathbb{F}_2) \cdot < \alpha^{2^{\frac{n}{4}}+1} >$.

Remark

Since $\gcd(d, 2^m - 1) = 1$ if m is odd, x^d is a permutation of $\mathbb{F}_{2^m}$.

CCK Case : $d = 2^{\frac{n}{3}} + 2^{\frac{n}{6}} + 1$, $n = 0 \mod 6$

Theorem (Canteaut - Charpin - Kyureghyan, 2008)

$\mathcal{B}_d = \{u \in \mathbb{F}^\star_{2^{\frac{n}{2}}} \mid Tr_{\frac{n}{6}}^{\frac{n}{2}}(u) = 0\} \cdot \{x^d, x \in \mathbb{F}^\star_{2^n}\}$

Theorem

There is no bent functions of the form $Tr_{\frac{n}{2}}^{n}(ax^d)$.

Theorem

Let m be a divisor of n such that $m < \frac{n}{2}$. Then, $Tr_m^n(ax^d)$ is bent if and only if $a \in \{u \in \mathbb{F}^\star_{2^{\frac{n}{2}}} \mid Tr_{\frac{n}{6}}^{\frac{n}{2}}(u) = 0\} \cdot < \alpha^{\gcd(2^{\frac{n}{3}}+2^{\frac{n}{6}}+1, t)} >$.

Example

$Tr_4^{12}(abx^{21})$ is bent provided that $Tr_2^6(a) = 0$ with $a \in \mathbb{F}_{64}$ and b is the 21th-power of an element of $\mathbb{F}_{2^{12}}$ and x^{21} does not permutes $\mathbb{F}_{2^4}$.

Dillon Case : $d = r(2^{\frac{n}{2}} - 1)$, $\gcd(r, 2^{\frac{n}{2}} + 1) = 1$

Theorem (Dillon, 1974, Charpin - Gong, 2008)

$\mathcal{B}_d = \{a \in \mathbb{F}_{2^n} \mid K_{\frac{n}{2}}(a^{2^{\frac{n}{2}}+1}) = 0\}$ *where*

$$K_{\frac{n}{2}}(u) = \sum_{x \in \mathbb{F}_{2^{\frac{n}{2}}}} (-1)^{Tr_1^n(ux + \frac{1}{x})}$$

is a Kloosterman sum.

Theorem

Suppose that $n = 2 \mod 4$ *and* $n \geq 6$*. Then,* $Tr_2^n(ax^d)$ *is bent if and only if* $K_{\frac{n}{2}}(a^{2^{\frac{n}{2}}+1}) = 0$

Theorem

There is no bent functions of the form $Tr_{\frac{n}{2}}^n(ax^d)$.

Problem

Does exist bent functions $Tr_m^n(ax^d)$ *with* $m \geq 3$ *and* $m \neq \frac{n}{2}$ *?*

Bent vectorial functions with multiple terms

n even integer, $m|n$, $m \leq \frac{n}{2}$

Vectorial functions with mutiple terms : $a_i \in \mathbb{F}_{2^n}$, d_i are integers

$$F(x) = \sum_{i=1}^{t} Tr_m^n(a_i x^{d_i})$$

Component functions :

$$Tr_1^m(uF(x)) = \sum_{i=1}^{t} Tr_1^n(a_i u x^{d_i})$$

Fact

Let $m|n$. Then, $F(x) = \sum_{i=1}^{t} Tr_m^n(a_i x^{d_i})$ is bent if and only if $f(x) = \sum_{i=1}^{t} Tr_1^n(c_i u x^{d_i})$ is bent for every $(c_1, \ldots, c_t) \in \prod_{i=1}^{t} a_i \mathbb{F}_{2^m}^\star$.

Bent vectorial functions with multiple terms: Niho exponents

$n = 2k$, k positive integer

Niho exponent : an exponent d is an Niho exponent if the restriction of x^d to $\mathbb{F}_{2^k}$ is linear

Niho exponent : $d = (2^k - 1)s + 2^v$

Vectorial function :

$$F(x) = \sum_{i=1}^{t} Tr_m^n\left(a_i x^{(2^k-1)s_i + 2^{v_i}}\right)$$

Component functions : $m|k$, $u \in \mathbb{F}_{2^m}^\star$. Thus, for every u and u' in $\mathbb{F}_{2^m}^\star$,

$$\begin{aligned} f_u(x) = Tr_1^m(uF(x)) &= \sum_{i=1}^{t} Tr_1^n(a_i u'((u/u')^{2^{-v_i}} x)^{(2^k-1)s_i+2^{v_i}}) \\ &= f_{u'}((u/u')^{2^{-v_i}} x) \end{aligned}$$

Bent vectorial functions with multiple terms : Niho exponents

Theorem

The vectorial function

$$\sum_{i=1}^{t} Tr_m^n\left(a_i x^{(2^k-1)s_i+2^{v_i}}\right)$$

are bent for every $m|k$ if and only if the Boolean function

$$f_1(x)=\sum_{i=1}^{t} Tr_1^n\left(a_i x^{(2^k-1)s_i+2^{v_i}}\right)$$

is bent.

Bent vectorial functions with multiple terms : Dillon exponents

$n = 2k$ even integer

Theorem (Li - Helleseth - Tang - Kolosha, 2013)

The Boolean function defined for any $x \in \mathbb{F}_{2^n}$ as

$$f(x) = \sum_{i=1}^{2^{k-2}} Tr_1^n\left(ax^{(2^i-1)(2^k-1)}\right)$$

is bent if and only if $a \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$.

Fact

$a\mathbb{F}_{2^m}^\star \subset \mathbb{F}_{2^k} \setminus \mathbb{F}_2$ if and only if $m \neq k$, $m|k$ and $a \in \mathbb{F}_{2^k} \setminus \mathbb{F}_{2^m}$.

Bent vectorial functions with multiple terms : Dillon exponents

$n = 2k$ even integer

Theorem

Let $m \neq k$, $m|k$ and $a \in \mathbb{F}_{2^k} \setminus \mathbb{F}_{2^m}$. The vectorial function

$$f(x) = \sum_{i=1}^{2^{k-2}} Tr_m^n \left(a x^{(2^i-1)(2^k-1)} \right)$$

is bent

Bent vectorial functions with multiple terms : a particular case

Theorem (Muratovic-Ribic - Pasalic - Bajric, 2014)

Let $n \geq 4$ and $m|k$. let x^{d_1} be a permutation of $\mathbb{F}_{2^m}$ and $\sum_{i=1}^{t} Tr_1^n(a_i x^{d_1+v_i(2^m-1)})$ be a Boolean bent function, where v_i are positive integers. Then, the vectorial function $\sum_{i=1}^{t} Tr_m^n(a_i x^{d_1+v_i(2^m-1)})$ is bent.

We show that, in some situations, we can relax the condition that x^{d_1} is a permutation and exhibit vectorial functions of the above form but with a weaker condition on x^{d_1} that is, that its range set is equal to $\mathbb{F}_{2^m}$.

Upper bounds on the nonlinearity of S-boxes

$m > \frac{n}{2}$

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_{2^m}^\star;\ u \in \mathbb{F}_{2^n}} |W_F(u,v)|$$

Covering radius bound :

$$nl(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

SCV bound, Sidelnikov-Chabaud-Vaudenay :

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \times 2^n - 2 - 2 \cdot \frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}$$

less than the covering radius bound only if $m > n-1$ and achieved only if $m = n$ odd : F almost bent function, $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$.

Upper bounds on the nonlinearity of S-boxes

Carlet-Ding bound, 2007 : $m < 2^n - 2$

$$nl(F) \leq 2^{n-1} - \frac{m2^{n-2}}{2^{n-1}-1}$$

- Does not improve the covering radius bound if $m \leq n-1$
- Is better than the SCV bound if

$$m^2 \left(\frac{2^{n-1}-1}{2^{n-1}} \right)^2 + 2 \cdot \frac{(2^n-1)(2^{n-1}-1)}{2^m-1} > 3 \times 2^n - 2$$

Balancedness

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

$F^{-1}(b) = \{a \in \mathbb{F}_{2^n} \mid F(a) = b\}$, $b \in \mathbb{F}_{2^m}$

$|A|$ = cardinality of A

Definition

F is said to be balanced if and only if $|F^{-1}(b)| = 2^{n-m}$ for every $b \in \mathbb{F}_{2^m}$.

Imbalance

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Remark

$$\frac{1}{2^m} \sum_{b \in \mathbb{F}_{2^m}} \left|F^{-1}(b)\right| = 2^{n-m}$$

Imbalance of a vectorial function (Carlet-Ding, 2004):

$$Nb_F = \sum_{b \in \mathbb{F}_{2^m}} \left(\left|F^{-1}(b)\right| - 2^{n-m}\right)^2$$

Fact

$Nb_F = 0$ *if and only F is balanced.*

Imbalance

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Remark

The imbalance of F is preserved under the composition at left or at right by an affine automorphisms likewise the nonlinearity nl :

$$Nb_{A_1 \circ F \circ A_2} = Nb_F \quad \text{and} \quad nl(A_1 \circ F \circ A_2) = nl(F)$$

for every vectorial function $F ; \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $A_1 \in AGL(\mathbb{F}_{2^m})$ and $A_2 \in AGL(\mathbb{F}_{2^n})$.

Imbalance

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Remark

$nl(F + A) = nl(F)$ for every affine function : $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

On the other hand :

- The imbalance is preserved under the addition of a constant function : $Nb_F = Nb_{F+c}$ for every $c \in \mathbb{F}_{2^m}$
- the imbalance is not invariant under the addition of a linear function : Nb_{F+L} and Nb_F can differ for some linear functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

A first upper bound involving the imbalance of the derivatives of F

$$D_aF(x) = F(x) + F(x+a)$$

$$NB_F = \sum_{a \neq 0} Nb_{D_aF}$$

Theorem (Carlet - Ding, 2007)

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{2^{m-n}}{2^m - 1} NB_F}$$

A second upper bound on the nonlinearity involving Nb_F

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Theorem (Carlet, 2011)

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^m}{2^m - 1} Nb_F}$$

Remark

If F is bent then $Nb_F = 2^n - 2^{n-m}$ and Carlet's bound coincides with the covering radius bound.

An upper bound on the nonlinearity involving Nb_F

$\mathcal{L}_{n,m} = \{L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}, L \text{ linear}\}$

Corollary (Carlet, 2011)

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^m}{2^m - 1} \max_{L \in \mathcal{L}_{n,m}} Nb_{F+L}}$$

Remark

$$\frac{1}{|\mathcal{L}_{m,n}|} \sum_{L \in \mathcal{L}_{n,m}} Nb_{F+L} = 2^n - 2^{n-m}$$

Thus :

$$\frac{2^m}{2^m - 1} \max_{L \in \mathcal{L}_{n,m}} Nb_{F+L} \geq 2^n$$

A new upper bound

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Theorem

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{2^{2m-n}\left(Nb_F - (2^n - 2^{n-m})\right)^2}{(2^n-1)(2^m-1)^2}}$$

Fact

If F is bent then $Nb_F = 2^n - 2^{n-m}$

A new upper bound

Fact

Lower than Carlet's bound if

$$Nb_F \leq 2^n - 2^{n-m}$$

or, if $m \leq n$,

$$Nb_F \geq 2^n - 2^{n-m} + 2^{2m-2n}(2^n-1)(2^m-1)$$

A new upper bound

$$\mathcal{L}_{n,m} = \{L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}, L \text{ linear}\}$$

Remark

For every $L \in \mathcal{L}_{n,m}$,

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{2^{2m-n}\left(Nb_{F+L} - (2^n - 2^{n-m})\right)^2}{(2^n-1)(2^m-1)^2}}$$

Fact

The variance of Nb_{F+L} as L ranges $\mathcal{L}_{n,m}$ is equal to $2^{-m}\sum_{a\in\mathbb{F}_{2^n}^\star} Nb_{D_aF}$.

A second upper bound

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Theorem

If there exists $u \neq 0$ in $\mathbb{F}_{2^n}$ such that $Tr_1^n(ux)$ is constant on each set $F^{-1}(b)$, then we have:

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{2n} + 2^m Nb_F}{2^m - 1}} < 2^{n-1} - 2^{n-\frac{m}{2}-1}.$$

Remark

- if $n > m$, smaller than the covering radius bound and Carlet-Ding bound
- Does not apply to every vectorial functions. Relaxing the condition on F, that is, supposing that the Hamming weight of $u \cdot x$ lies outside a weight range, leads to a weaker upper bound.

On bent components of vectorial function

$n = 2k$, k positive integer

$F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$

$$\mathcal{B}_F = \{a \in \mathbb{F}_{2^n}^{\star} \mid Tr_1^n(aF) \text{ is bent}\}$$

Example (Niho power function)

$F(x) = x^{2^k+1}$, $\mathcal{B}_F = \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, $|B_F| = 2^n - 2^k$.

Theorem (Pott - Pasalic - Muratovic-Ribic - Bajric, 2017)

For any $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, $|B_F| \leq 2^n - 2^k$.

On bent components of vectorial function

Theorem (Pott - Pasalic - Muratovic-Ribic - Bajric, 2017)

Let F and F' be two vectorial functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Suppose that F and F' are EA-equivalent. Then $|\mathcal{B}_F| = 2^n - 2^k$ if and only if $|\mathcal{B}_{F'}| = 2^n - 2^k$.

Theorem

Let F and F' be two vectorial functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Suppose that F and F' are CCZ-equivalent. Then $|\mathcal{B}_F| = 2^n - 2^k$ if and only if $|\mathcal{B}_{F'}| = 2^n - 2^k$.

On bent components of vectorial function

$F(x) = x^{2^i}(x + x^{2^k})$, i nonnegative integer

Theorem (Pott - Pasalic - Muratovic-Ribic - Bajric, 2017)
$Tr_1^n(aF(x))$ is bent if and only if $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$.

Fact

- *All bent functions $Tr_1^n(aF)$ are in the Maiorana-McFarland class.*
- *F is CCZ-inequivalent to x^{2^k+1}.*

On bent components of vectorial function

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $F(x) = xL(x)$, $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, linear

Problem

Determine the linear maps L for which the so-defined vectorial function F has the maximum number of bent components.

Lemma

Let L be a linear map from $\mathbb{F}_{2^n}$ to itself. $L^\star$ denotes the adjoint map of L : $Tr_1^n(xL(y)) = Tr_1^n(L^\star(x)y)$.
Then $f(x) = Tr_1^n(xL(x))$ is bent if and only if $x \mapsto L(x) + L^\star(x)$ is invertible.

On bent components of vectorial function

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $F(x) = x^{2^i} L(x)$, L linear

Problem

Determine L such that $x \mapsto aL^{2^{-i}}(x) + L^\star(a^{2^i} x^{2^i})$ is invertible for **exactly** $2^n - 2^k$ *values of a.*

Theorem

Let t_1 and $t-2$ be two integers. Suppose that $z^{2^{k-t1}-1} + z^{2^{k-t2}-1} + 1$ and $z^{2^{t_1}-1} + z^{2^{t_2}-1} + 1$ have no roots in $\mathbb{F}_{2^k}$. Then

$$L(x) = x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_2}} + x^{2^{t_1+k}} + x^{2^{t_2+k}}$$

is a solution of the problem