Bent and Plateaued Functions for Symmetric Cryptography: insights and open problems

Sihem Mesnager

Department of Mathematics, University of Paris VIII
and University Sorbonne Paris Cité, LAGA, CNRS,
and Telecom Paris, Polytechnic Institute of Paris, France

Young Researchers Algebra Conference 2023
July 28, 2023, L'Aquila, Italy

- In 1966 : the first paper written by Oscar Rothaus (published in 1976).
- In 1972 and 1974 : two documents written by John Dillon.
- In 1975 : a paper based on Dillon's thesis.
- In this preliminary period, several people were interested in bent functions, particularly Lloyd Welch and Gerry Mitchell.
- It seems that bent functions have been studied by V.A. Eliseev and O.P. Stepchenkov in the Soviet Union already in 1962, under the name of *minimal functions*. Some results were published as technical reports but never declassified.

Outline

1. Boolean functions, bentness and related notions
2. Characterizations and properties of bent functions
3. Bent functions : applications
4. Equivalence, classification and enumeration of bent functions
5. Primary and secondary constructions of Boolean bent functions
6. Bent functions and their variance (subclasses, extensions, generalizations)

Let q be a power of a prime p and r be a positive integer. The trace function $Tr_{q^r/q} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is defined as :

$$Tr_{q^r/q}(x) := \sum_{i=0}^{r-1} x^{q^i} = x + x^q + x^{q^2} + \cdots + x^{q^{r-1}}.$$

The trace function from $\mathbb{F}_{q^r} = \mathbb{F}_{p^n}$ to its prime subfield $\mathbb{F}_p$ is called the *absolute trace* function.

☞ Here, we shall use the following notation in characteristic 2 :

DEFINITION (ABSOLUTE TRACE OVER $\mathbb{F}_2$)

Let k be a positive integer. For $x \in \mathbb{F}_{2^k}$, the (absolute) trace $Tr_1^k(x)$ of x over $\mathbb{F}_2$ is defined by :

$$Tr_1^k(x) := \sum_{i=0}^{k-1} x^{2^i} = x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}} \in \mathbb{F}_2$$

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ an n-variable Boolean function.

Definition (Algebraic Normal Form (A.N.F))

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then f can be expressed as :

$$f(x_1, \ldots, x_n) = \bigoplus_{I \subset \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u, a_I \in \mathbb{F}_2$$

where $I = \mathrm{supp}(u) = \{i = 1, \ldots, n \mid u_i = 1\}$ *and* $x^u = \prod_{i=1}^{n} x_i^{u_i}$.

The A.N.F exists and is unique.

Definition (The algebraic degree)

The algebraic degree $\deg(f)$ *is the degree of the A.N.F.*

Affine functions f $(\deg(f) \leq 1)$:

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n, \; a_i \in \mathbb{F}_2$$

DEFINITION

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its ***polynomial form :***

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n - 1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

- Γ_n is the set obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$,
- $o(j)$ is the size of the cyclotomic coset containing j (that is $o(j)$ is the smallest positive integer such that $j2^{o(j)} \equiv j \pmod{2^n - 1}$)
- $\epsilon = wt(f)$ modulo 2

DEFINITION (THE HAMMING WEIGHT OF A BOOLEAN FUNCTION)

$$wt(f) = \#supp(f) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$$

Definition

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its ***polynomial form*** *:*

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n - 1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

☞ **The algebraic degree** of f denoted by $\deg(f)$, is the maximum Hamming weight of the binary expansion of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

- Affine functions : $Tr_1^n(ax) + \lambda$, $a \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_2$.

DEFINITION (THE BIVARIATE REPRESENTATION (UNIQUE))

Let $n = 2m$*, let* $\mathbb{F}_2^n \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$*.*

$$f(x,y) = \sum_{0 \le i,j \le 2^m-1} a_{i,j} x^i y^j;\ a_{i,j} \in \mathbb{F}_{2^m}$$

.

- Then the algebraic degree of f equals $\max_{(i,j)\,|\,a_{i,j}\neq 0}(w_2(i) + w_2(j))$.
- And f being Boolean, its bivariate representation can be written in the form $f(x,y) = Tr_1^m(P(x,y))$ where $P(x,y)$ is some polynomial over $\mathbb{F}_{2^m}$.

The discrete Fourier (Walsh) Transform of Boolean functions

Definition (The discrete Fourier (Walsh) Transform)

$$\widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot x}, \quad a \in \mathbb{F}_2^n$$

where "$\cdot$" is the canonical scalar product in $\mathbb{F}_2^n$ defined by
$x \cdot y = \sum_{i=1}^{n} x_i y_i, \forall x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, \quad \forall y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n.$

Definition (The discrete Fourier (Walsh) Transform)

$$\widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(ax)}, \quad a \in \mathbb{F}_{2^n}$$

where "Tr_1^n" is the absolute trace function on $\mathbb{F}_{2^n}$.

Definition (The discrete Fourier (Walsh) Transform)

$$\widehat{\chi_f}(a, b) = \sum_{x, y \in \mathbb{F}_{2^m}} (-1)^{f(x,y) + Tr_1^m(ax + by)}, \quad a, b \in \mathbb{F}_{2^m}.$$

Definition (The Hamming distance)

$f, g : \mathbb{F}_{2^n} \to \mathbb{F}_2$ two Boolean functions. The Hamming distance between f and g : $d_H(f,g) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) \neq g(x)\}$.

Definition (Nonlinearity)

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ a Boolean function. The nonlinearity denoted by $\mathrm{nl}(f)$ of f is

$$\mathrm{nl}(f) := min_{l \in A_n} d_H(f, l)$$

where $A_n := \{l : \mathbb{F}_{2^n} \to \mathbb{F}_2, \quad l(x) := a \cdot x + b\,;\, a \in \mathbb{F}_{2^n}, \quad b \in \mathbb{F}_2$ (where "$\cdot$" is an inner product in $\mathbb{F}_{2^n}$)} is the set of affine functions on $\mathbb{F}_{2^n}$.

➔ The nonlinearity of a function f is the minimum number of truth table entries that must be changed in order to convert f to an affine function.
☛ Any cryptographic function must be of high nonlinearity, to prevent the system from linear attacks and correlation attacks.

The Nonlinearity of f is equals :

$$\mathrm{nl}(f) \;=\; 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |\widehat{\chi_f}(a)|$$

➔Thanks to Parseval's relation : $\sum_{a\in\mathbb{F}_2^n} \widehat{\chi_f}^{\,2}(a) = 2^{2n}$
we have : $\max_{a\in\mathbb{F}_2^n} \left(\widehat{\chi_f}(a)\right)^2 \geq 2^n$

Hence : for every n-variable Boolean function f, the nonlinearity is always upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$

➔It can reach this value if and only if n is even.

➔ The functions used as combining or filtering functions should have nonlinearity close to this maximum.

- **General upper bound on the nonlinearity of any n-variable Boolean function :**$\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$

Definition (Bent function [Rothaus, 1975])

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *(n even) is said to be a bent function if* $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$

Bent functions have been studied for more than 40 years (initiators : [Dillon, 1974], [Rothaus, 1975]).

- **A main characterization of "bentness" :**

$$(f \text{ is bent }) \iff \widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}, \quad \forall \omega \in \mathbb{F}_{2^n}$$

Parseval's identity allows one to determine the number of occurrences of each value of the Walsh transform of a bent function.

Table – Walsh spectrum of bent functions f with $f(0) = 0$

Value of $\widehat{\chi_f}(\omega)$, $\omega \in \mathbb{F}_{2^n}$	Number of occurrences
$2^{\frac{n}{2}}$	$2^{n-1} + 2^{\frac{n-2}{2}}$
$-2^{\frac{n}{2}}$	$2^{n-1} - 2^{\frac{n-2}{2}}$

Let f be a Boolean function over $\mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}$. The derivative of f with respect to a is defined as :

$$D_a f(x) = f(x) + f(x+a); x \in \mathbb{F}_{2^n}.$$

For $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, the *second-order derivative* of f with respect (a,b) is defined as :

$$D_b D_a f(x) = D_b(D_a f)(x) = f(x) + f(x+b) + f(x+a) + f(x+a+b), \forall x \in \mathbb{F}_{2^n}.$$

The *linear kernel of* f is the linear subspace of vectors a such that $D_a f$ is a constant function. Any element of the linear kernel is called a *linear structure* of f.

☞ A function f is bent if and only if all the derivatives $D_a f$, $a \in \mathbb{F}_{2^n}^\star$, are balanced (Dillon reports that D. Lieberman has first observed this).

Bent functions : applications

From a cryptographic viewpoint, bent functions have two main interests :

1. Their *derivatives* $D_af : x \mapsto f(x) + f(x+a)$ are balanced, therefore any addition of a nonzero vector to the input to f induces 2^{n-1} changes among the 2^n outputs ; this has an important relationship with the differential attack on block ciphers, which was already known at the NSA in the seventies.
2. The Hamming distance between f and the set of affine Boolean functions takes optimal value $2^{n-1} - 2^{\frac{n}{2}-1}$ (n even) ; this has a direct relationship with the fast correlation attack [Meier-Staffelbach 1988] on stream ciphers and the linear attack [Matsui 1993] on block ciphers.

Two main drawbacks :

1. Bent functions are not balanced and can hardly be used, for instance, in stream ciphers.
2. A pseudo-random generator using a bent function as a combiner or filter is weak against some attacks, like the fast algebraic attack [Courtois 2003], even if the bent function has been modified to make it balanced, as Dobbertin described.

Let q be a prime power and n be a positive integer.

Definition

The support of a vector $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ *is defined as* $supp(a) := \{0 \leq i \leq n-1 : a_i \neq 0\}$. *The Hamming weight of* $a \in \mathbb{F}_q^n$*, denoted by* $wt(a)$*, is the cardinality of its support, i.e.,* $wt(a) := \#supp(a)$.

Definition (Linear codes)

A linear $[n, k, d]_q$ *code* $\mathcal{C}$ *over a field* $\mathbb{F}_q$ *is a* k*-dimensional subspace of* $\mathbb{F}_q^n$ *with minimum Hamming distance* d *with* $d := d(\mathcal{C}) = min_{\bar{a},\bar{b} \in \mathcal{C}, \bar{a} \neq \bar{b}} d(\bar{a}, \bar{b})$ *where the distance* $d(\bar{a}, \bar{b})$ *between two vectors* $\bar{a}$ *and* $\bar{b}$ *is the number of coordinates in which they differ.*

Bent functions and covering radius of Reed-Muller codes

$\mathcal{B}_n = \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$

- The Reed-Muller code $\mathcal{RM}(r,n)$ can be defined in terms of **Boolean functions** : $\mathcal{RM}(r,n)$ is the set of all n-variable Boolean functions $\mathcal{B}_n$ of algebraic degrees at most r. More precisely, it is the linear code of all binary words of length 2^n corresponding in the truth tables of these functions.
- For every $0 \leq r \leq n$, the Reed-Muller code $\mathcal{RM}(r,n)$ of order r, is a linear code :

$$\left[\underbrace{2^n}_{length}, \underbrace{\sum_{i=0}^{r}\binom{n}{i}}_{dimension}, _{minimum}\underbrace{2^{n-r}}_{distance}\right]$$

A cryptographic parameter for Boolean functions : the r th-order nonlinearity

DEFINITION (r-TH-ORDER NONLINEARITY : $nl_r(f)$ ($r \in \mathbb{N}$, $r \leq n$))

The r-th order nonlinearity *of* f *is the minimum Hamming distance between* f *and the set of all the* n*-variable Boolean functions of algebraic degree at most* r : $nl_r(f) = \min_{g \in \mathcal{RM}(r,n)} d_H(f,g)$

The r th-order nonlinearity $nl_r(f)$ generalizes the (standard) nonlinearity $nl(f)$ and is an important parameter in cryptography : it measures the capacity for resisting low-degree approximation attack.

- ☞ We were interested in the maximal value of $nl_r(f)$ $(r > 1)$ of n-variable Boolean functions f

Covering radius of the Reed-Muller code $\mathcal{RM}(r,n)$

☞ The maximal nonlinearity of order r of n-variable Boolean functions coincides with the covering radius of $\mathcal{RM}(r,n)$.

DEFINITION (COVERING RADIUS OF THE REED-MULLER CODE $\mathcal{RM}(r,n)$)

Covering radius of the Reed-Muller code $\mathcal{RM}(r,n)$ of order r and length 2^n :

$$\bullet \rho(r,n) := \max_{f\in\mathcal{B}_n} \min_{g\in\mathcal{RM}(r,n)} d_H(f,g) = \max_{f\in\mathcal{B}_n} nl_r(f)$$

where $\mathcal{B}_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$. Or :

$$\bullet \rho(r,n) := \min\{d \in \mathbb{N} \mid \cup_{x\in\mathcal{RM}(r,n)} B(x,d) = \mathbb{F}_2^n\}$$

where $B(x,d) := \{y \in \mathbb{F}_2^n \mid d_H(x,y) \le d\}$ (Hamming ball)

Bent functions and covering radius of Reed-Muller codes

- ☞ The covering radius plays an important role in error correcting codes : measures the maximum errors to be corrected in the context of maximum-likelihood decoding.
- ☞ The best upper bound of $\rho(r,n)$ $(r>1)$ ([Carlet-SM, 2007]).

- When n is odd, $\rho(1,n) < 2^{n-1} - 2^{\frac{n}{2}-1}$
- When n is even, $\rho(1,n) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and the associated n-variable Boolean functions are the bent functions.

Bent functions are combinatorial objects :

DEFINITION

- *Let G be a finite (abelian) group of order μ. A subset D of G of cardinality k is called (μ, k, λ)-difference set in G if every element $g \in G$, different from the identity, can be written as $d_1 - d_2$, $d_1, d_2 \in D$, in exactly λ different ways.*
- *Hadamard difference set in elementary abelian 2-group :* $(\mu, k, \lambda) = (2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$.

THEOREM (DILLON 74)

A Boolean function f over $\mathbb{F}_2^n$ is bent if and only if $supp(f) := \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ is a Hadamard difference set in $\mathbb{F}_2^n$.

Example : Let f a Boolean function defined on $\mathbb{F}_2^4$ $(n = 4)$ by $f(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3$ The support of f is $Supp(f) = \{(1,0,0,1),(1,0,1,1),(1,1,0,1),(0,1,1,0),(0,1,1,1),(1,1,1,0)\}$ is a Hadamard $(16, 6, 2)$-difference set of $\mathbb{F}_2^4$.

d_1	d_2	$d_1 + d_2$
1001	1011	0010
1001	1101	0100
1001	0110	1111
1001	0111	1110
1001	1110	0111
1011	1101	0110
1011	0110	1101
1011	0111	1100
1011	1110	0101
1101	0110	1011
1101	0111	1010
1101	1110	0011
0110	0111	0001
0110	1110	1000
0111	1110	1001

Bent functions : properties, classification, enumeration

Main properties of bent functions :

- if f is bent then $wt(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.
- If f is bent then $\widehat{\chi_f}(\omega) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(\omega)}$, for all $\omega \in \mathbb{F}_2^n$, defines the dual function $\tilde{f}$ of f.

  -It has been also shown by [Carlet 1999] that, denoting by $\mathcal{F}(f)$ the character sum $\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}$, and by ℓ_a the linear form $\ell_a(x) = a \cdot x$, we have : $\mathcal{F}(D_a\widetilde{f} + \ell_b) = \mathcal{F}(D_bf + \ell_a)$.
  -It is shown by [Hou 2000] that the algebraic degrees of any n-variable bent function and of its dual satisfy :

$$m - \deg f \geq \frac{m - \deg \widetilde{f}}{\deg \widetilde{f} - 1}.$$

- If f is bent then $\deg f \leq \frac{n}{2}$

Recall that the algebraic degree of any bent function on $\mathbb{F}_{2^n}$: $\deg(f) \leq \frac{n}{2}$.
Therefore, for any bent Boolean function f defined over $\mathbb{F}_{2^n}$:

- Polynomial form :

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) \quad , a_j \in \mathbb{F}_{2^{o(j)}}$$

  - Γ_n is the set obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$,
  - $o(j)$ is the size of the cyclotomic coset containing j,

Equivalence :

DEFINITION

Two Boolean functions f and f' defined on $\mathbb{F}_{2^n}$ are called extended affine equivalent (EA-equivalent) if $f' = f \circ \phi + \ell$ where the mapping ϕ is an affine automorphism on $\mathbb{F}_{2^n}$ and ℓ is an affine Boolean function .

- ☞ The bentness is an affine invariant.
- ☞ All bent quadratic functions are EA-equivalent.
- ☞ There exist other equivalence notions coming from design theory [Dillon 1974, Kantor 1975, Dillon-Schatz 1987].

Classification and enumeration :

There does not exist for $n \geq 10$ a classification of bent functions under the the action of the general affine group.

☞ The classification of bent functions for $n \geq 10$ and even counting them are still wide-open problems.

- The number of bent functions is known for $n \leq 8$ (the number of 8-variable bent functions has been found recently [Langevin-Leander-Rabizzoni-Veron-Zanotti 2008]).

n	2	4	6	8
$\#$ of bent functions	$8 = 2^3$	$896 = 2^{9.8}$	$5,425,430,528$	
$\approx$			$2^{32.3}$	$2^{106.3}$

- Only bounds on their number are known (cf. [Carlet-Klapper 2002]).
- The problem of determining an efficient lower bound on the number of n-variable bent functions is open.

Bent functions : constructions

- To understand better the structure of bent functions, we can try to design constructions of bent functions. It is also useful to deduce constructions of highly nonlinear balanced functions.
- Some of the known constructions of bent functions are direct ; that is, do not use previously constructed bent functions as building blocks. We will call primary constructions these direct constructions. The others, sometimes leading to recursive constructions, will be called secondary constructions.

- **Maiorana-Mc Farland's class $\mathcal{M}$** : the best-known construction of bent functions defined in bivariate form (explicit construction). $f_{\pi,g}(x,y) = x \cdot \pi(y) + g(y)$, with $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a permutation and $g : \mathbb{F}_2^m \to \mathbb{F}_2$ any mapping.
- **Dillon's Partial Spreads class $\mathcal{PS}^-$** : well-known construction of bent functions whose bentness is achieved under a condition based on a decomposition of its supports (not explicit construction) : $supp(f) = \bigcup_{i=1}^{2^{m-1}} E_i^\star$ where $\{E_i, 1 \leq i \leq 2^{m-1}\}$ are m-dimensional subspaces with $E_i \cap E_j = \{0\}$.
- **Dillon's Partial Spreads class $\mathcal{PS}_{ap}$** : a subclass of $\mathcal{PS}^-$'s class. Functions in $\mathcal{PS}_{ap}$ are defined explicitly in bivariate form : $f(x,y) = g(xy^{2^m-2})$ with g is a balanced Boolean function on $\mathbb{F}_{2^m}$ which vanishes at 0.
- **Dillon's class H** : a nice original construction of bent functions in bivariate representation but less known because Dillon could only exhibit functions that already belonged to the well-known Maiorana-McFarland class. The bentness is achieved under some non-obvious conditions. The class H has been extended ([Carlet-SM, 2010]).

Partial spreads and spreads

Partial spreads and spreads play an important role in some constructions of bent functions.

Definition (Partial spread)

For a group G of order M^2, a partial spread is a family $S = \{H_1, H_2, \cdots, H_N\}$ of subgroups of order M which satisfy $H_i \cap H_j = \{0\}$ for all $i \neq j$.

Definition (Spread)

With the previous notation, if $N = M + 1$ (which implies $\cup_{i=1}^{M+1} H_i = G$) then S is called a spread.

- We will call the subgroups of a spread also spread elements.

DEFINITION ($\frac{n}{2}$-SPREAD)

Let $n = 2m$ be an even integer. An m-spread of $\mathbb{F}_{2^n}$ is a set of pairwise supplementary m-dimensional subspaces of $\mathbb{F}_{2^n}$ whose union equals $\mathbb{F}_{2^n}$

Hence a collection $\{E_1, \cdots, E_s\}$ of $\mathbb{F}_{2^n}$ is an m-spread of $\mathbb{F}_{2^n}$ $(n = 2m)$ if

1. $E_i \cap E_j = \{0\}$ for $i \neq j$;
2. $\bigcup_{i=1}^{s} E_i = \mathbb{F}_{2^n}$;
3. $dim_{\mathbb{F}_2} E_i = m$, $\forall i \in \{1, \cdots, s\}$.

Example (A classical example of m-spread : the Desarguesian spread)

Let consider the additive group $(\mathbb{F}_{p^n}, +)$ of the finite field $\mathbb{F}_{p^n}$ with $n = 2m$.

- (In univariate form) Let $S_1 := \{u_i\mathbb{F}_{p^m}, i = 1, \cdots, p^m + 1\}$ where $\{u_i \mid i = 1, \cdots, p^m + 1\}$ is the set of representatives of the cosets of the subgroup $\mathbb{F}^\star_{p^m}$ of the multiplicative group $\mathbb{F}^\star_{p^n}$. S_1 is a spread of $\mathbb{F}_{p^n}$.
- (In bivariate form) Let S_2 be the family of subgroups of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ given by $S_2 = \cup_{s\in\mathbb{F}_{p^m}}\{(x, sx) \mid x \in \mathbb{F}_{p^m}\} \cup \{(0, y), y \in \mathbb{F}_{p^m}\}$. S_2 is a spread of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Example (The Desarguesian m-spread (in characteristic 2))

- in $\mathbb{F}_{2^n}$: $\{u\mathbb{F}_{2^m}, u \in U\}$ where $U := \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$
- in $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$: $\{E_a, a \in \mathbb{F}_{2^m}\} \cup \{E_\infty\}$ where $E_a := \{(x, ax) ; x \in \mathbb{F}_{2^m}\}$ and $E_\infty := \{(0, y) ; y \in \mathbb{F}_{2^m}\} = \{0\} \times \mathbb{F}_{2^m}$.

Partial Spread ($\mathcal{PS}$) class

Let $\{E_1, \cdots, E_s\}$ be a partial spread of $\mathbb{F}_{2^n}$ and f a Boolean function over $\mathbb{F}_{2^n}$. Assume that
$f = \sum_{i=1}^{s} 1_{E_i} - 2\lfloor \frac{s}{2} \rfloor \delta_0$, 1_{E_i} are the the indicators of the E_i's and δ_0 is the Dirac symbol.
We have : f is then bent if and only if

1. $s = 2^{m-1}$ (in which case f is said to be in the $\mathcal{PS}^-$ class)
2. or $s = 2^{m-1} + 1$ (in which case f is said to be in the $\mathcal{PS}^+$ class).

Dillon introduces in a family of bent functions that he denotes by H, whose bentness is achieved under some non-obvious conditions. He defines these functions in bivariate form (but they can also be seen in univariate form). The functions of this family are defined as $f(x, y) = Tr_1^m(y + xG(yx^{2^m-2}))$; $x, y \in \mathbb{F}_{2^m}$; where G is a permutation of $\mathbb{F}_{2^m}$ such that $G(x) + x$ does not vanish and, for every $\beta \in \mathbb{F}_{2^m}^{\star}$, the function $G(x) + \beta x$ is two-to-one.

Extension of the class H of Dillon :

Definition (Class $\mathcal{H}$-Carlet-SM 2011)

We call $\mathcal{H}$ the class of functions f defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$f(x,y) = Tr_1^m(\mu y + xG(yx^{2^m-2}))$$

with

1. $G : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ *is a permutation ;*
2. $\forall \beta \in \mathbb{F}_{2^m}^{\star}$*, the function* $z \mapsto G(z) + \beta z$ *is 2-to-1 on* $\mathbb{F}_{2^m}$.

- Functions f in the class $\mathcal{H}$ are whose restrictions to elements of the m-spread $\{E_a, E_\infty\}$ are linear
- The class H of Dillon is a subclass of $\mathcal{H}$. Indeed, if we take (in the definition of functions in class $\mathcal{H}$) $\mu = 1$ and G such that $G(z) + z$ does not vanishes then, we get functions in H.

A first contribution thanks to the introduction of the class $\mathcal{H}$:

- ☞ Functions of class $\mathcal{H}$ in univariate form are the known *Niho* bent functions.

PROPOSITION

A Boolean function $f(x) = \sum_{d=0}^{2^n-2} a_d x^d$ ($f(0) = 0$) has linear restrictions to the $u\mathbb{F}_{2^m}$'s if and only if all exponents d such that $a_d \neq 0$ are congruent with powers of 2 modulo $2^m - 1$. An integer d is said to be an exponent of type Niho if $d \equiv 2^i \pmod{2^m - 1}$. Niho-bent functions are bent functions in which their polynomial form involves exponents of type Niho.

Functions in the previous proposition have already been investigated as *Niho bent functions.*

Known bent functions of type Niho :

1. one monomial (that is, if the form $x \mapsto Tr_1^n(ax^s)$ where s is a Niho exponent).
2. three binomials (that is, if the form $x \mapsto Tr_1^n(a_1x^{s_1} + a_2x^{s_2})$, where s_1 and s_2 are two Niho exponents).
3. one multinomial (that is, of the form $x \mapsto \sum_i Tr_1^n(a_ix^{s_i})$ where s_i are Niho

A second contribution thanks to the introduction of the class $\mathcal{H}$:

PROPOSITION ([CARLET-SM 2012])

Let G satisfies the condition :
$\forall \beta \in \mathbb{F}_{2^m}^\star$, *the function* $z \mapsto G(z) + \beta z$ *is 2-to-1 on* $\mathbb{F}_{2^m}$. *if and only if for every* $\gamma \in \mathbb{F}_{2^m}$, *the function* $H_\gamma : z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} \text{ if } z \neq 0 \\ 0 \text{ if } z = 0 \end{cases}$ *is a permutation on* $\mathbb{F}_{2^m}$.

- Note that if H_γ is a permutation on $\mathbb{F}_{2^m}$ then G is a permutation on $\mathbb{F}_{2^m}$.

Definition

Let m be any positive integer. A permutation polynomial G over $\mathbb{F}_{2^m}$ is called an o-polynomial if, for every $\gamma \in \mathbb{F}_{2^m}$, the function H_γ :

$$z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$$ *is a permutation on $\mathbb{F}_{2^m}$.*

The notion of o-polynomial comes from Finite Projective Geometry :

☞ There is a close connection between "o-polynomials" and "hyperovals" :

Definition (A hyperoval of $PG_2(2^n)$)

Denote by $PG_2(2^n)$ the projective plane over $\mathbb{F}_{2^n}$.
A hyperoval of $PG_2(2^n)$ is a set of $2^n + 2$ points no three collinear.

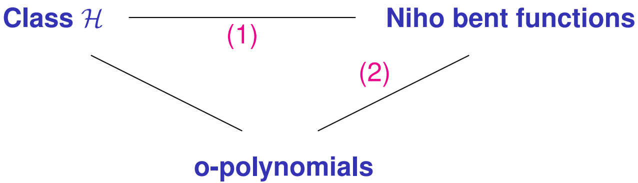
A hyperoval of $PG_2(2^n)$ can then be represented by
$D(f) = \{(1, t, f(t)), t \in \mathbb{F}_{2^n}\} \cup \{(0, 1, 0), (0, 0, 1)\}$ or
$D(f) = \{(f(t), t, 1), t \in \mathbb{F}_{2^n}\} \cup \{(0, 1, 0), (1, 0, 0)\}$ where f is an o-polynomial.

☞ There exists a list of only 9 classes of o-polynomials found by the geometers in 40 years

Class $\mathcal{H}$, Niho bent functions and o-polynomial

To summarize :

Class $\mathcal{H}$ (bent functions in bivariate forms ; contains a class H introduced by Dillon in 1974).



1. The correspondence (1), offers a new framework to study the properties of Niho bent functions. We have used a such framework to answer many questions left open in the literature. Further open problems are still left open.
2. Thanks to the connection (2) and thanks to the results of the geometers (obtained in 40 years), we can construct several potentially new families of bent functions in $\mathcal{H}$ and thus new bent functions of type Niho.

Main secondary constructions (1/5) :

- The direct sum : if f and g are bent in n and r variables respectively, then $f(x)+g(y)$, $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^r$, is bent as well.
- Rothaus' construction which uses three initial n-variable bent functions h_1, h_2, h_3 to build an $n+2$-variable bent function f : let $x \in \mathbb{F}_2^n$ and $x_{n+1}, x_{n+2} \in \mathbb{F}_2$; let $h_1(x)$, $h_2(x)$, $h_3(x)$ be bent functions on $\mathbb{F}_2^n$ such that $h_1(x)+h_2(x)+h_3(x)$ is bent as well, then the function defined at every element (x, x_{n+1}, x_{n+2}) of $\mathbb{F}_2^{n+2}$ by :

$$\begin{aligned} f(x, x_{n+1}, x_{n+2}) = & \, h_1(x)h_2(x) + h_1(x)h_3(x) + h_2(x)h_3(x) \\ & + [h_1(x)+h_2(x)]x_{n+1} + [h_1(x)+h_3(x)]x_{n+2} \\ & + x_{n+1}x_{n+2} \end{aligned}$$

  is a bent function in $n+2$ variables.

Main secondary constructions (1/5)

- The indirect sum and its generalizations : use four bent functions : let f_1, f_2 be bent on $\mathbb{F}_2^r$ (r even) and g_1, g_2 be bent on $\mathbb{F}_2^s$ (s even) ; define

$$h(x,y) = f_1(x) + g_1(y) + (f_1 + f_2)(x)\,(g_1 + g_2)(y),\ x \in \mathbb{F}_2^r,\ y \in \mathbb{F}_2^s, \quad (1)$$

then h is bent and

$$\widetilde{h}(x,y) = \widetilde{f}_1(x) + \widetilde{g}_1(y) + (\widetilde{f}_1 + \widetilde{f}_2)(x)\,(\widetilde{g}_1 + \widetilde{g}_2)(y),\ x \in \mathbb{F}_2^r,\ y \in \mathbb{F}_2^s.$$

☞ Two generalizations of the indirect sum needing initial conditions are given and a modified indirect sum is also introduced

Main secondary constructions (1/5)

- A construction without extension of the number of variables([Carlet 2006]) :
  Let f_1, f_2 and f_3 be three Boolean functions on $\mathbb{F}_2^n$. Consider the Boolean functions $s_1 = f_1 + f_2 + f_3$ and $s_2 = f_1 f_2 + f_1 f_3 + f_2 f_3$ (sums performed in $\mathbb{F}_2$). Then

$$\widehat{\chi_{f_1}} + \widehat{\chi_{f_2}} + \widehat{\chi_{f_3}} = \widehat{\chi_{s_1}} + 2\,\widehat{\chi_{s_2}} \quad (2)$$

  (sums performed in $\mathbb{Z}$), and if f_1, f_2 and f_3 are bent then :
  1. if s_1 is bent and if $\tilde{s_1} = \tilde{f_1} + \tilde{f_2} + \tilde{f_3}$, then s_2 is bent, and $\tilde{s_2} = \tilde{f_1}\tilde{f_2} + \tilde{f_1}\tilde{f_3} + \tilde{f_2}\tilde{f_3}$;
  2. if $\widehat{\chi_{s_2}}(a)$ is divisible by 2^m for every a (*e.g.* if s_2 is bent), then s_1 is bent.
  It has been observed in [SM 2014] that the converse of 1. is also true : if f_1, f_2, f_3 and s_1 are bent, then s_2 is bent if and only if $\tilde{f_1} + \tilde{f_2} + \tilde{f_3} + \tilde{s}_1 = 0$.

Main secondary constructions (1/5)

- There exist also bent functions associated with some vectorial (n, n)-functions called almost bent (AB). Almost bent functions are those vectorial (n, n)-functions having maximal nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ (n odd). Given such function F, the indicator γ_F of the set $\{(a, b) \in (\mathbb{F}_2^n \setminus \{0\}) \times \mathbb{F}_2^n;\ \exists x \in \mathbb{F}_2^n,\ F(x) + F(x + a) = b\}$ is a bent function. The known AB power functions $F(x) = x^d$, $x \in \mathbb{F}_{2^m}$ are given in Table 2.

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, m) = 1,\ 1 \leq i < m/2$
Kasami-Welch	$2^{2i} - 2^i + 1$	$\gcd(i, m) = 1,\ 2 \leq i < m/2$
Welch	$2^k + 3$	$m = 2k + 1$
Niho	$2^k + 2^{\frac{k}{2}} - 1$, k even $2^k + 2^{\frac{3k+1}{2}} - 1$, k odd	$m = 2k + 1$

Table – Known AB power functions x^d on $\mathbb{F}_{2^m}$.

Main secondary constructions (1/5) The bent functions γ_F associated to known AB functions :

- *Gold :* $\gamma_F(a,b) = Tr_1^m(\frac{b}{a^{2^i+1}})$ with $\frac{1}{0} = 0$;
- *Kasami-Welch, Welch, Niho* : we have $F(x+1) + F(x) = q(x^{2^s} + x)$, $\gcd(s,m) = 1$, where q is in each case a permutation determined by Dobbertin and $F(x+1) + F(x) = b$ has solutions if and only if $Tr_1^m(q^{-1}(b)) = 0$. Then :

$$\gamma_F(a,b) = \begin{cases} Tr_1^m(q^{-1}(b/a^d)) + 1 & \text{if } a \neq 0, \\ 0 & \text{otherwise} ; \end{cases}$$

  Some specific values of s and q have been investigated (Kasami-Welch, Welch and Niho).

The functions γ_F associated to Kasami-Welch, Welch and Niho functions with $m = 7, 9$, are neither in completed $\mathcal{M}$ class, nor in completed $\mathcal{PS}_{ap}$ class.
The other known infinite classes of AB functions are quadratic ; their associated γ_F belong to completed $\mathcal{M}$ class.

Primary constructions in univariate trace form (1/2)

- $f(x) = Tr_1^n\left(ax^{2^j+1}\right)$, where $a \in \mathbb{F}_{2^n} \setminus \{x^{2^j+1};\, x \in \mathbb{F}_{2^n}\}$, $\frac{n}{gcd(j,n)}$ even
  This class has been generalized to functions of the form
  $Tr_1^n(\sum_{i=1}^{m-1} a_i x^{2^i+1}) + c_m Tr_1^m(a_m x^{2^m+1})$, $a_i \in \mathbb{F}_2$.
- $f(x) = Tr_1^n\left(ax^{2^{2j}-2^j+1}\right)$, where $a \in \mathbb{F}_{2^n} \setminus \{x^3;\, x \in \mathbb{F}_{2^n}\}$, $gcd(j,n) = 1$
- $f(x) = Tr_1^n\left(ax^{(2^{n/4}+1)^2}\right)$, where $n \equiv 4$ [mod 8], $a = a'b^{(2^{n/4}+1)^2}$,
  $a' \in w\mathbb{F}_{2^{n/4}}$, $w \in \mathbb{F}_4 \setminus \mathbb{F}_2$, $b \in \mathbb{F}_{2^n}$;
- $f(x) = Tr_1^n\left(ax^{2^{n/3}+2^{n/6}+1}\right)$, where $6\,|\,n$, $a = a'b^{2^{n/3}+2^{n/6}+1}$, $a' \in \mathbb{F}_{2^m}$,
  $Tr_{m/3}^m(a') = 0$, $b \in \mathbb{F}_{2^n}$;
- $f(x) = Tr_1^n\left(a[x^{2^i+1} + (x^{2^i} + x + 1)Tr_1^n(x^{2^i+1})]\right)$, where $n \geq 6$, m does not divide i, $\frac{n}{\mathrm{gcd}(i,n)}$ even, $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^i}$,
  $\{a, a+1\} \cap \{x^{2^i+1};\, x \in \mathbb{F}_{2^n}\} = \emptyset$;
- $f(x) = Tr_1^n\Big(a\Big[\Big(x + Tr_3^n\big(x^{2(2^i+1)} + x^{4(2^i+1)}\big)$
  $+Tr_1^n(x)Tr_3^n\big(x^{2^i+1} + x^{2^{2i}(2^i+1)}\big)\Big)^{2^i+1}\Big]\Big)$ (under some conditions).

Primary constructions in univariate trace form (2/2)

- The 5 known classes of Niho bent functions ;
- 3 classes of bent (in fact, hyper-bent) functions via Dillon-like exponents and others coming from their generalizations : Dillon's and generalized Dillon's functions, 2 classes by SM and their generalizations ;
- Bent functions have been also obtained by Dillon and McGuire as the restrictions of functions on $\mathbb{F}_{2^{n+1}}$, with $n+1$ odd, to a hyperplane of this field.

Known infinite classes of bent functions in bivariate trace form

- Functions from the Maiorana McFarland class $\mathcal{M}$;
- Functions from Dillon's $\mathcal{PS}_{ap}$;
- An isolated class : $f(x,y) = Tr_1^m(x^{2^i+1} + y^{2^i+1} + xy)$, $x, y \in \mathbb{F}_{2^n}$ where n is co-prime with 3 and i is co-prime with m ;
- Bent functions in a bivariate representation related to Dillon's H class obtained from the known o-polynomials ;
- Bent functions associated to AB functions ;
- Several new infinite families of bent functions and their duals ;
- Several new infinite families of bent functions from new permutations and their duals ;
- Several new infinite families of bent functions from involutions and their duals.

☞ Other primary constructions of bent functions have been obtained as restrictions and extensions.

Bent functions and their variance (subclasses, extensions, generalizations)

Definition (hyper-bent Boolean function [Youssef-Gong 01])

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be a hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime to $2^n - 1$.

Characterization : f is hyper-bent on $\mathbb{F}_{2^n}$ if and only if its extended Hadamard transform takes only the values $\pm 2^{\frac{n}{2}}$.

Definition (The extended discrete Fourier (Walsh) Transform)

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega, k) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\omega x^k)}, \text{ with } \gcd(k, 2^n - 1) = 1.$$

- Hyper-bent functions were initially proposed by [Golomb-Gong 1999] as a component of S-boxes to ensure the security of symmetric cryptosystems.
- Hyper-bent functions have properties stronger than bent functions ; they are rarer than bent functions.

☞ Hyper-bent functions are used in S-boxes (DES).

The most relevant results on hyper-bent functions are related to Dillon bent functions from partial spreads.
Primary constructions and characterizations of hyper-bent functions in univariate form have been made for (Dillon exponent : $r(2^m - 1)$)

1. Monomial hyper-bent functions via Dillon exponents ([Dillon 1975]) ;
2. Binomial hyper-bent functions via Dillon exponents ([Mesnager 2009])
3. Multimonomial hyper-bent functions via Dillon exponents ([Charpin-Gong 2008, Mesnager 2010, Mesnager-Flori 2012]).
4. Very recently, [Tang-Qi 2014] have identified hyperbent functions by considering a particular form of functions with Dillon exponents over $\mathbb{F}_{2^{2m}}$.

- ☞ A new criterion [Canteaut-Rotella, 2016] given on filtered LFSRs has revived the interest in hyper-bent functions.
- ☞ New results on (p-ary and generalized) hyper-bent functions [Mesnager, 2020].

Notation

We denote by $\mathcal{D}_n$ the set of bent functions f defined on $\mathbb{F}_{2^n}$ by $f(x) = \sum_i Tr_{2^{o(j)}/2}(a_i x^{d_i})$ with $\forall i, d_i \equiv 0 \pmod{2^m - 1}$ such that $f(0) = 0$.

- All the known constructions of hyper-bentness are obtained for functions in $\mathcal{D}_n$.
- [SM-Mandal-Tang, 2020] provided characterizations of the hyper-bentness property and a new algorithm method to construct (but complex !) hyper-bent Boolean functions

- An (n,r)-function $F:\mathbb{F}_2^n \mapsto \mathbb{F}_2^r$ being given, the component functions of F are the Boolean functions $l \circ F$, where l ranges over the set of all the nonzero linear forms over $\mathbb{F}_2^r$. Equivalently, they are the functions of the form $v \cdot F,\ v \in \mathbb{F}_2^r \setminus \{0\}$, where "$\cdot$" denotes an inner product in $\mathbb{F}_2^r$.
- The vector spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^r$ can be identified, if necessary, with the Galois fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^r}$ of orders 2^n and 2^r respectively.
- Hence, (n,r)-functions can be viewed as functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^r$ or as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$. In the latter case, the component functions are the functions $Tr_1^r(vF(x))$.

Because of the linear cryptanalysis and the fast correlation attack on stream ciphers, the notion of nonlinearity has been generalized to (n, r)-functions and studied by [Nyberg 1991-1993] and further studied by [Chabaud-Vaudenay 1995].

- F is bent if and only if all of its component functions are bent ; equivalently, $\widehat{\chi_{v \cdot F}}(a) = \pm 2^m$ for all $a \in \mathbb{F}_2^n$ and all $v \in \mathbb{F}_2^r \setminus \{0\}$.
- Hence, F is bent if and only if, for every $v \in \mathbb{F}_2^r \setminus \{0\}$ and every $a \in \mathbb{F}_2^n \setminus \{0\}$, the function $v \cdot (F(x) + F(x + a))$ is balanced. An (n, r)-function F is balanced (*i.e.* takes every value of $\mathbb{F}_2^r$ the same number 2^{n-r} of times) if and only if all its components are balanced.
- F is then bent if and only if, for every $a \in \mathbb{F}_2^n$, the derivative $F(x) + F(x + a)$ of F is balanced.

In characteristic p (p prime), the trace function $Tr_{p^k}^{p^n}$ from the finite field $\mathbb{F}_{p^n}$ of order p^n to the subfield $\mathbb{F}_{p^k}$ is defined as

$$Tr_{p^k}^{p^n} = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ki}}.$$

For $k = 1$ we have the absolute trace and use the notation $tr_n(\cdot)$ for $Tr_p^{p^n}(\cdot)$.
A p-ary function is a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$.

- $\mathbb{F}_p^n \approx \mathbb{F}_{p^n}$, a p-ary functions can be described in the so-called *univariate form*, which is a unique polynomial over $\mathbb{F}_{p^n}$ of degree at most $p^n - 1$ or in *trace form* $tr_n(F(x))$ for some function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ (non unique).
- A p-ary function has a representation as a unique multinomial in $x_1, \cdots, x_n$, where the variables x_i occur with exponent at most $p-1$. This is called the *multivariate representation* or ANF.

The Walsh-Hadamard transform can be defined for p-ary functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$:

$$S_f(b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x) - tr_n(bx)},$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ is the complex primitive p^{th} root of unity and elements of $\mathbb{F}_p$ are considered as integers modulo p.

DEFINITION

A p-ary function f is called bent if all its Walsh-Hadamard coefficients satisfy $|S_f(b)|^2 = p^n$. A bent function f is called regular bent if for every $b \in \mathbb{F}_{p^n}$, $p^{-\frac{n}{2}} S_f(b) = \zeta_p^{f^\star(b)}$ for some p-ary function $f^\star : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

DEFINITION

The bent function f is called weakly regular bent if there exists a complex number u with $|u| = 1$ and a p-ary function $f^\star$ such that $up^{-\frac{n}{2}} S_f(b) = \zeta_p^{f^\star(b)}$ for all $b \in \mathbb{F}_{p^n}$. Weakly regular bent functions allow construction of strongly regular graphs and association schemes.

Walsh-Hadamard transform coefficients of a p-ary bent function f with odd p satisfy

$$p^{-\frac{n}{2}} S_f(b) = \begin{cases} \pm\zeta_p^{f^\star(b)}, & \text{if } n \text{ is even or } n \text{ is odd and } p \equiv 1 \pmod 4, \\ \pm i\zeta_p^{f^\star(b)}, & \text{if } n \text{ is odd and } p \equiv 3 \pmod 4, \end{cases} \tag{3}$$

where i is a complex primitive 4-th root of unity. Therefore, regular bent functions can only be found for even n and for odd n with $p \equiv 1 \pmod 4$. Moreover, for a weakly regular bent function, the constant u (defined above) can only be equal to ± 1 or $\pm i$.

Bent functions	m	p
$\sum_{i=0}^{\lfloor m/2 \rfloor} Tr_{p^m/p}(a_i x^{p^i+1})$	arbitrary	arbitrary
$\sum_{i=0}^{p^k-1} Tr_{p^m/p}(a_i x^{i(p^k-1)}) + Tr_{p^l/p}(\delta x^{\frac{p^m-1}{e}})$, $e \mid p^k+1$	$m = 2k$	arbitrary
$Tr_{p^m/p}(a x^{\frac{3^m-1}{4}+3^k+1})$	$m = 2k$	$p = 3$
$Tr_{p^m/p}(x^{p^{3k}+p^{2k}-p^k+1} + x^2)$	$m = 4k$	arbitrary
$Tr_{p^m/p}(a x^{\frac{3^i+1}{2}})$; i odd, $gcd(i,m) = 1$	arbitrary	$p = 3$

Table – Known weakly regular bent functions over $\mathbb{F}_{p^m}$, p odd

- in [Tang, Li, Qi, Zhou, Helleseth, 2016], introduced a very interesting special class $\mathcal{RF}$ of p-ary weakly regular bent functions such that $f(0) = 0$; and there exists an integer h such that $(h-1, p-1) = 1$ and $f(cx) = c^h f(x)$ for any $c \in \mathbb{F}_p^*$ and $x \in \mathbb{F}_{p^n}^*$.
- all the known weakly regular bent functions belong to $\mathcal{RF}$. Recently [Du, Jin, SM 2021] completed results from [Xu, Cao, Xu, 2017] and we obtained some constructions of p-ary weakly regular bent functions (outside $\mathcal{RF}$) :
    - $f(x) = \mathrm{Tr}_1^m(\lambda x^{p^m+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)^l$, for all $n = 2m$ and $\lambda \in \mathbb{F}_{p^m}^*$,
    - $f(x) = \mathrm{Tr}_1^n(\lambda_1 x^2) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)^l$, for all integers $n > 2$ and $\lambda_1 \in \mathbb{F}_{p^n}^*$,
    - $f(x,y) = \mathrm{Tr}_1^m(x\pi(y)) + \mathrm{Tr}_1^m(y) + \mathrm{Tr}_1^m(u_1x + u_2y)\mathrm{Tr}_1^m(v_1x + v_2y)^l$, where $l \in \{p-1, \frac{p-1}{2}\}$, $u, v \in \mathbb{F}_{p^n}^*$ such that u, v are not both in $\mathbb{F}_p$, π is a linearized permutation polynomial over $\mathbb{F}_{p^m}$ and $(u_1, u_2), (v_1, v_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Problem : find new strategies to derive new weakly regular bent functions

Vectorial (plateaued) p-ary functions can be defined as follows.

- A p-ary function is called a *plateaued function* if the Walsh transform W_f takes at most three values. Because of Parseval identify, $|W_f(a)|^2 \in \{0, \mu^2\}$ where $\mu^2 = p^{n+s}$ for some positive integer s such that $0 \leq s \leq n$. The power $\mu := p^{\frac{n+s}{2}}$ is called the amplitude of f and we say that f is an s-*plateaued*.
- Bent functions are the 0-plateaued.
- A vectorial function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is called *vectorial plateaued* if all its components F_u from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ (defined by $F_u(x) = Tr_{p^m/p}(uF(x))$ for every $x \in \mathbb{F}_{p^n}$) are s_u-plateaued for every $u \in \mathbb{F}_{p^m}^\star$ with possibly different amplitudes. In particular, F is called *vectorial* s-*plateaued* if F_u are s-plateaued with the same amplitude μ for every $u \in \mathbb{F}_{p^m}^\star$.

We have the following main results :

- Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an s-plateaued function. Then for $\omega \in \mathbb{F}_{p^n}$, $|W_f(\omega)|^2$ takes p^{n-s} times the value p^{n+s} and $p^n - p^{n-s}$ times the value 0 ([SM 2014]).
- It have shown by [Hyun-Lee-Lee, 2016] that the Walsh transform coefficients of p-ary s-plateaued f satisfy

$$W_f(a) = \begin{cases} \pm p^{\frac{n+s}{2}} \zeta_p^{g(a)}, 0 & \text{if } n+s \text{ is even or} \\ & \quad n+s \text{ is odd and } p \equiv 1 \pmod 4, \\ \pm i p^{\frac{n+s}{2}} \zeta_p^{g(a)}, 0 & \text{if } n+s \text{ is odd and } p \equiv 3 \pmod 4, \end{cases} \tag{4}$$

where i is a complex primitive 4-th root of unity and g is a p-ary function over $\mathbb{F}_{p^n}$ with $g(a) = 0$ for all $a \in \mathbb{F}_{p^n} \setminus supp(W_f)$ (recall : the support of a vectorial function $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ is the set $Supp(F) := \{x \in \mathbb{F}_{q^n} \mid f(x) \neq 0\}$.)

[SM, Özbudak, Sınak, 2017] have introduced the notion of weakly regular plateaued functions in odd characteristic, which covers a non-trivial subclass of the class of plateaued functions.

- Let p be an odd prime and $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary s-plateaued function, where s is an integer with $0 \leq s \leq n$. Then, f is called *weakly regular p-ary s-plateaued* if there exists a complex number u such that $|u| = 1$ and u does not depend on ω. such that $W_f(\omega) \in \left\{0, up^{\frac{n+s}{2}} \xi_p^{g(\omega)}\right\}$ for all $\omega \in \mathbb{F}_{p^n}$, where g is a p-ary function over $\mathbb{F}_{p^n}$ with $g(\omega) = 0$ for all $\omega \in \mathbb{F}_{p^n} \setminus supp(W_f)$;
- otherwise, f is called *non-weakly regular p-ary s-plateaued*.
- In particular, weakly regular p-ary s-plateaued f is called *regular p-ary s-plateaued* when $u = 1$.

Examples : let $\mathbb{F}_{2_{3^3}}^{\star} = \langle \zeta \rangle$ with $\zeta^3 + 2\zeta + 1 = 0$.

- $f(x) = Tr_{3^3/3}(\zeta^5 x^{11} + \zeta^{20} x^5 + \zeta^{11} x^4 + \zeta^2 x^3 + \zeta x^2)$ is regular 3-ary 1-plateaued over $\mathbb{F}_{2_{3^3}}$
- The function $f(x) = Tr_{3^3/3}(\zeta x^{13} + \zeta^7 x^4 + \zeta^7 x^3 + \zeta x^2)$ is weakly regular 3-ary 1-plateaued over $\mathbb{F}_{2_{3^3}}$.
- The function $f(x) = Tr_{3^3/3}(\zeta^{16} x^{13} + \zeta^2 x^4 + \zeta^2 x^3 + \zeta x^2)$ is non-weakly regular 3-ary 2-plateaued over $\mathbb{F}_{2_{3^3}}$.

It has been shown by [SM, Özbudak,Sınak, 2017] that :

- Let p be an odd prime and $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a weakly regular s-plateaued function. For all $\omega \in supp(W_f)$, $W_f(\omega) = \epsilon\sqrt{p^*}^{n+s}\zeta_p^{g(\omega)}$, where $\epsilon = \pm 1$ is the sign of W_f, p^* denotes $\left(\frac{-1}{p}\right)p$ (where $(\frac{\cdot}{\cdot})$ denotes the Legendre symbol) and g is a p-ary function over $supp(W_f)$.

For p-ary plateaued functions (any prime p), we have a lot of characterizations [Carlet, SM, Meidl, Özbudak, Sınak, etc.], some properties but quite very few constructions [Hodzic, Pasalic, Wei, Zhang 2019], [SM, Özbudak,Sınak, 2021] , etc.
Generic constructions are necessary !
Problem : Find (primary) constructions plateaued functions and, more importantly, generic constructions !

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ (resp. $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$) :

☞ Families of functions according to the spectrum of values of W_f (resp. W_F) : bent and their variants.

- f bent : $|W_f(a)| = p^{n/2}, \forall a \in \mathbb{F}_{p^n}$
- F vectorial bent : all the components $Tr_{p^m/p}(bF(x))$, $b \neq 0$, are bent
- f weakly regular bent : $W_f(\lambda) = \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(\lambda)}$, $\varepsilon = \pm 1$
- F almost bent (AB) : $W_F(a,b) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^n}$
- f plateaued : W_f takes at most 3 values $|W_f(a)| \in \{0, \mu\}$ for all $a \in \mathbb{F}_{p^n}$
- F plateaued : all the components $Tr_{p^m/p}(bF(x))$, $b \neq 0$, are plateaued
- f weakly regular s-plateaued : $W_f(a) \in \{0,\ up^{\frac{m+s}{2}} \zeta_p^{g(a)}\}$, $|u| = 1$
- F plateaued of amplitude μ : all the components $Tr_{p^m/p}(bF(x))$, $b \neq 0$ are plateaued of amplitude μ