Bent functions and their connections to coding theory and cryptography

Sihem Mesnager

University of Paris VIII and University of Paris XIII
Department of mathematics,
LAGA (Laboratory Analysis, Geometry and Application), CNRS,
Telecom Paristech, France

Fifteenth International Conference on Cryptography and Coding

IMACC 2015
Oxford, United Kingdom
15th December 2015

Bent functions

- 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, in particular 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 constructions of Boolean bent functions
6. Secondary constructions of Boolean bent functions
7. Bent functions in univariate and bivariate representations
8. Subclasses, super-classes of bent functions
9. Vectorial bent functions
10. p-ary functions and bentness
11. Constructions of bent functions in arbitrary characteristic

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ 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 :***

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

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 :

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

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))

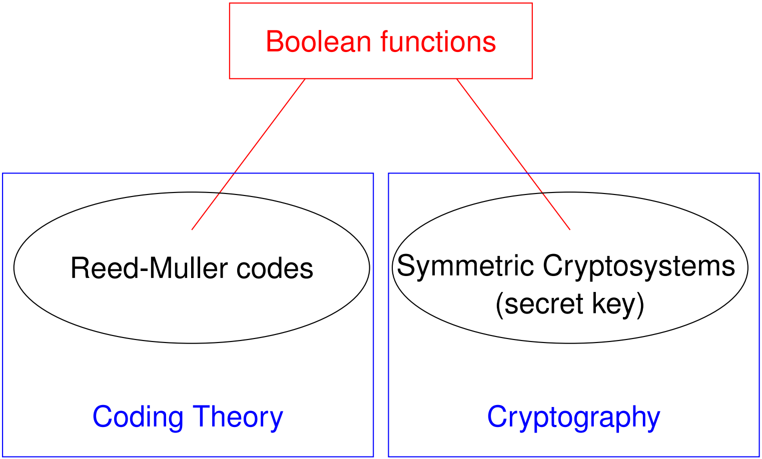
Let $n = 2m$, *let* $\mathbb{F}_2^n \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

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

.

- Then the algebraic degree of f equals $\max_{(i,j) \mid a_{i,j} \neq 0} (w_2(i) + w_2(j))$.
- 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 $\mathbb{F}_{2^m}$.

☞ In both **Error correcting coding** and **Symmetric cryptography**, Boolean functions are important objects !



☞ To make the cryptanalysis very difficult to implement, we have to pay attention when choosing the Boolean function, that has to follow several recommendations : **cryptographic criteria** !

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 : $\max_{a\in\mathbb{F}_2^n} (\widehat{\chi_f}(a))^2 \geq 2^n$

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" :**

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

Thanks to Parseval's identity, one can 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 :

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

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

Bent functions : applications

Two main interests :

1. Their *derivatives* $D_a f : x \mapsto f(x) + f(x+a)$ are balanced, this has an important relationship with the differential attack on block ciphers.
2. The Hamming distance between f and the set of affine Boolean functions takes optimal value ; 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 then can hardly be used for instance in stream ciphers.
2. A pseudo-random generator using a bent function as 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.

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 Covering radius $\rho(1,n)$ of the Reed-Muller code $\mathcal{RM}(1,n)$ coincides with the maximum nonlinearity $nl(f)$.
- General upper bound on the nonlinearity : $\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$

- 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.

1. It is well-known that Kerdock codes are constructed from bent functions. Moreover, bent functions can also be used to construct linear codes [Ding 2014] with few weights [Tang-Li-Qi-Zhou-Helleseth 2015, Mesnager 2015]. Such codes have applications in secret sharing, authentication codes, regular graphs.
2. Bent functions can be used to construct codebooks derived from codes [Xiang-Ding-Mesnager 2015]. Codebooks achieving some bounds are used in direct spread CDMA systems, quantum information processing, packing and coding theory.
3. Bent functions play a role even in very practical issues through the so-called robust error detecting codes.

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

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 $\mathbb{F}_2^n$.

We can define the square $2^n \times 2^n$ matrix whose term at row indexed by $x \in \mathbb{F}_2^n$ and column indexed by $y \in \mathbb{F}_2^n$ equals $(-1)^{f(x+y)}$; then, f is bent if and only if this matrix is a Hadamard matrix (i.e. has mutually orthogonal rows). So bent functions play a role in designs (any difference set can be used to construct a symmetric design), sequences for communications, etc.

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].
- There exists a related open question [Tokareva 2011] : are all Boolean functions of algebraic degrees at most m the sums of two bent functions ?

Classification and enumeration :

There does not exist for $n \geq 10$ a classification of bent functions under 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

Some of the known constructions of bent functions are direct, that is, do not use as building blocks previously constructed bent functions. 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 $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ 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 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. The bentness is achieved under some non-obvious conditions. It was extended by [Carlet-Mesnager 2011] : **class $\mathcal{H}$**.

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 (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 $E_\infty := \{(0, y)\,;\, y \in \mathbb{F}_{2^m}\} = \{0\} \times \mathbb{F}_{2^m}$.

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
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).

The union of $\mathcal{PS}^+$ and $\mathcal{PS}^-$ forms the partial spread class $\mathcal{PS}$.
Dillon introduced this important class, which represents numerous functions [Dembowski 1968, Johnson-Jha-Biliotti 2007, Kantor 2003]).

- Dillon has also introduced bent functions obtained using, more generally, sets of subgroups of a group. This extension to subgroups has been pushed further in [Hou 1988, Kantor 2012].
- It has also been shown that the work of Dillon can be extended to odd characteristic [Lisonek-Lu 2014, Mesnager 2015].
- Recently, finite pre-quasifield spreads from finite geometry have been revisited by Wu [Wu 2013]. In particular, Wu has considered the Dempwolff-Muller pre-quasifields, the Knuth pre-semifields and the Kantor pre-semifields to obtain the expressions of the $\mathcal{PS}$ corresponding bent functions.
- Very recently, [Carlet 2015] has similarly studied in the $\mathcal{PS}$ functions related to the André spreads and given the trace representation of the $\mathcal{PS}$ corresponding bent functions and of their duals.

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-Mesnager 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 $2^m - 1$.

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 exponents).

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

PROPOSITION ([CARLET-MESNAGER 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.

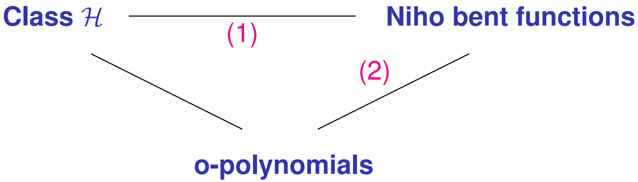
A hyperoval of $PG_2(2^n)$ can then be represented by
$D(f) = \{(1, t, f(t)), t \in \mathbb{F}_{2^n}\} \cup \{(0, 1, 0), (0, 0, 1)\}$ or
$D(f) = \{(f(t), t, 1), t \in \mathbb{F}_{2^n}\} \cup \{(0, 1, 0), (1, 0, 0)\}$ where f is an o-polynomial.

- 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 $s_2 = f_1f_2 + f_1f_3 + f_2f_3$ (sums performed in $\mathbb{F}_2$). Then

$$\widehat{\chi_{f_1}} + \widehat{\chi_{f_2}} + \widehat{\chi_{f_3}} = \widehat{\chi_{s_1}} + 2\,\widehat{\chi_{s_2}} \tag{2}$$

  (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 [Mesnager 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)

- Almost bent (AB) 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	$\gcd(i,m)=1,\ 1\le i<m/2$
Kasami-Welch	$2^{2i}-2^i+1$	$\gcd(i,m)=1,\ 2\le i<m/2$
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 $\mathbb{F}_{2^m}$.

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, $\frac{n}{\gcd(i,n)}$ 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 Mesnager 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 [Carlet 2008] ;
- Bent functions in a bivariate representation related to Dillon's H class obtained from the known o-polynomials [Carlet-Mesnager 2011] ;
- Bent functions associated to AB functions [Carlet-Charpin-Zinoviev 1998] ;
- Several new infinite families of bent functions and their duals [Mesnager IEEE 2014] ;
- Several new infinite families of bent functions from new permutations and their duals [Mesnager CCDS 2015] ;
- Several new infinite families of bent functions from involutions and their duals [Mesnager CCDS 2015].

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

Bent functions : subclasses, super-classes

Definition (hyper-bent Boolean function [Youssef-Gong 2001])

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (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)

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

- Hyper-bent functions were initially proposed by Golomb and Gong [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], etc.).
4. Very recently, [Tang-Qi 2014] have identified hyperbent functions by considering a particular form of functions with Dillon exponents over $\mathbb{F}_{2^{2m}}$.

Rotation symmetric bent functions and idempotent bent functions

- Rotation symmetric (RS) Boolean functions [Pieprzyk-Qu 1999] are those Boolean functions which are invariant under cyclic shifts of input coordinates : $f(x_{n-1}, x_0, x_1, \ldots, x_{n-2}) = f(x_0, x_1, \ldots, x_{n-1})$.
- RS Boolean functions are linked to a notion of idempotent [Filiol-Fontaine 1998-1999].
- Two infinite classes of quadratic RS functions and two infinite classes of cubic RS bent functions [Ma-Lee-Zhang 2005,Gao-Zhang-Liu-Carlet 2011,Carlet-Gao-Liu 2014] have been identified as well as their related idempotent functions.

Homogeneous bent functions

A bent function is called *homogeneous* if all the monomials of its algebraic normal form have the same degree.

- [Qu-Seberri-Pieprzyk 2000] had enumerated the 30 homogeneous bent functions of degree 3 in 6 variables and posed the problem of classifying the homogeneous bent functions in more variables.
- In [Charnes-Rotteler-Beth 2002] showed how to use invariant theory to construct homogeneous bent functions and proved that there exist homogeneous cubic bent functions for $n > 2$
- Using difference sets, [Xia et al. 2004] have proved that there exists no homogeneous bent function of degree m in $2m$ variables for $m > 3$.
- In [Meng et al. 2007], the authors have made this result precise by obtaining a bound on the degree of homogenous bent functions and proved that, for any non-negative integer k, there exists a positive integer N such that, for $n \geq N$, there exists no homogeneous bent function in $2n$ variables having degree $n - k$ or more, where N is the least integer satisfying a condition involving k.

For a given Boolean function f on $\mathbb{F}_2^n$:

$$N_{\Delta_f} \times N_{\widehat{\chi_f}} \geq 2^n, \tag{3}$$

where N_{Δ_f} denotes the cardinality of $\left\{b \in \mathbb{F}_2^n \mid \Delta_f(b) := \sum_{x\in\mathbb{F}_2^n}(-1)^{D_f(b)} \neq 0\right\}$ and $N_{\widehat{\chi_f}}$ denotes the cardinality of $\{b \in \mathbb{F}_2^n \mid \widehat{\chi_f}(b) \neq 0\}$.
It is known that $N_{\Delta_f} \times N_{\widehat{\chi_f}} = 2^n$ if and only if, for every $b \in \mathbb{F}_2^n$, the derivative $D_b f$ is either balanced or constant, and that this property is also equivalent to the fact that there exist two linear subspaces E (of even dimension) and E' of $\mathbb{F}_2^n$, whose direct sum equals $\mathbb{F}_2^n$, and Boolean functions g, bent on E, and h, affine on E', such that : $\forall x \in E,\ \forall y \in E', f(x+y) = g(x) + h(y)$. Such direct sum of a bent function and an affine function is called a *partially bent* function [Carlet 1993].

.

Definition (Zheng- Zhang 1999)

An n-variable Boolean function is called plateaued if its Walsh-Hadamard transform takes only one nonzero absolute value, and possibly the value 0.

Because of Parseval's relation, this can happen only with r-*plateaued* functions, for $0 \leq r \leq n$, where $n + r$ is even, whose Walsh-Hadamard transform values belong to the set $\{0, \pm 2^{\frac{n+r}{2}}\}$.

Applications in cryptography :

- Some plateaued functions have large nonlinearity, which provides protection against fast correlation attacks [Meier-Staffelbach 1988] when they are used as combiners or filters in stream ciphers, and contributes, when they are the component functions of the substitution boxes in block ciphers, to protection against linear cryptanalysis [Matsui 1994].
- They can also possess other desirable cryptographic characteristics.

The term *semi-bent function* has been introduced by [Chee-Lee -Kim 1994], but these functions had been previously called three-valued almost optimal Boolean functions.

Definition

Semi-bent functions (or 2-plateaued functions) over $\mathbb{F}_{2^n}$ satisfy $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$ and exist only when n is even.

Definition

Near-bent functions (or 1-plateaued functions) over $\mathbb{F}_{2^n}$ satisfy $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$ and exist only when n is odd.

- ☞ Survey in ["On semi-bent functions and related plateaued functions over the Galois field F_{2^n}". S. Mesnager. Proceedings "Open Problems in Mathematics and Computational Science", LNCS, Springer, pages 243-273, 2014.]

- 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 of 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.

Bent functions in characteristic p

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 constructing strongly regular graphs and association schemes.

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

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

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 $\pm i$.

Let p be a prime integer. A mapping F from $\mathbb{F}_{p^n}$ to itself is called *planar* if for any nonzero $b \in \mathbb{F}_{p^n}$, the mapping $F(x+b) - F(x)$ is bijective on $\mathbb{F}_{p^n}$.

☞ Every planar function gives a family of p-ary bent functions.

- We know only one example of a nonquadratic planar function known as Coulter-Matthews function which is defined over $\mathbb{F}_{3^n}$ by $F(x) = x^{\frac{3^k+1}{2}}$, with $gcd(k,n) = 1$ and k odd.
- All the other known planar functions are quadratic and can be represented as so-called Dembowski-Ostrom polynomials [Coulter-Matthews 1997].
- The bent functions coming from the Coulter-Matthews planar functions and from the (quadratic) p-ary bent functions $tr_n(aF)$ obtained from Dembowski-Ostrom polynomials are weakly regular bent.

- [Helleseth-Kholosha 2006] have exhibited a p-ary family of bent functions defined as follows : let f be the function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, $n = 2m$, defined as $f(x) = tr_n(ax^{r(p^m-1)})$, where p is an odd prime such that $p^m > 3$, r is an arbitrary positive integer such that $gcd(r, p^m + 1) = 1$ and $a \in \mathbb{F}_{p^n} \setminus \{0\}$,
- A ternary weakly regular bent function has been isolated and studied by several authors it is defined from $\mathbb{F}_{3^n}$ to $\mathbb{F}_3$ (where $n = 2m$ with m odd) by $f(x) = tr_n(ax^{\frac{3^n-1}{4}+3^m+1})$. The corresponding Walsh-Hadamard transform coefficient has been given.
- [Helleseth-Kholosha 2010] discovered a class of bent binomial functions : $f(x) = tr_n(x^{p^{3k}+p^{2k}-p^k+1} + x^2)$ for $n = 4k$. Such a class is the only infinite class of nonquadratic p-ary functions, in a univariate representation over fields of arbitrary odd characteristic, that has been proven to be bent.
- In 2013, several new classes of binary and p-ary regular bent functions (including binomials, trinomials, and functions with multiple trace terms) have been given by Li, Helleseth, Tang and Kholosha.

All bent functions in Table 3, possibly except for those of Dillon type, do not belong to the completed Maiorana-McFarland class.

n	d or $F(x)$	a	deg	Comments
	$\frac{3^k+1}{2}$, $gcd(k,n)=1$, k odd	$a \neq 0$	$k+1$	tern, R, WR
$2m$	$r(3^m-1)$, $gcd(r,3^m+1)=1$	$K_n^{(p)}(a^{3^m+1})=0$	n	tren, R
$2m$	$\frac{3^n-1}{4}+3^m+1$, m odd	$\zeta^{\frac{3^m+1}{4}}$	n	tern, WR
$4k$	$x^{p^{3k}+p^{2k}-p^k+1}+x^2$		$(p-1)k+2$	WR

TABLE: Nonquadratic p-ary Bent Functions

Tools for the study of the bentness :

- Tools from Galois fields
- Exponentials sums (Kloosterman sums, cubic sums, partial cubic sums, etc) ;
- Special polynomials (Dickson polynomials, Linearized polynomials, etc).
- Permutations mappings ;
- Hyperelliptic cuves ;
- etc.

Problems in this area amount to solve :

- an algebraic problem (linear algebra, etc) ;
- an arithmetical problem ;
- a problem related to exponential sums, Gauss sums, character sums, etc ;
- a problem from finite geometry ;
- a problem from algebraic geometry ;
- a combinatorial problem.

Example : a new construction of bent functions

Theorem (Mesnager-Cohen-Madore 2015)

Let n be an integer. Let d be a positive integer such that $d^2 \equiv 1 \pmod{2^n - 1}$. Let Φ_1, Φ_2 and Φ_3 be three mappings from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $\Phi_i(x) = \lambda_i x^d$ for all $i \in \{1, 2, 3\}$, where the $\lambda_i \in \mathbb{F}_{2^n}^\star$ are pairwise distinct such that $\lambda_i^{d+1} = 1$ and ${\lambda_0}^{d+1} = 1$, where $\lambda_0 := \lambda_1 + \lambda_2 + \lambda_3$. Let g be the Boolean function defined over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by

$$\begin{aligned} g(x,y) &= Tr_1^n(\Phi_1(y)x)Tr_1^n(\Phi_2(y)x) \\ &\quad + Tr_1^n(\Phi_2(y)x)Tr_1^n(\Phi_3(y)x) + Tr_1^n(\Phi_1(y)x)Tr_1^n(\Phi_3(y)x). \end{aligned}$$

Then the function g is bent and its dual is given by $\tilde{g}(x,y) = g(y,x)$.

The existence of bent functions given in the above theorem is a non-trivial arithmetical problem.

The arithmetical related problem

Given an odd positive integer e, we ask upon what conditions we can find n, d such that $d^2 \equiv 1 \pmod{2^n - 1}$ with $N/gcd(d+1, N) = e$ for $N := 2^n - 1$.

The algebraic related problem

We now turn to the "algebraic problem" : given e a positive odd integer and n such that e divides $N := 2^n - 1$, we wish to find $Z_0, \ldots, Z_3$ nonzero such that $Z_0^e + Z_1^e + Z_2^e + Z_3^e = 0$.

- ☞ The latter equation defines (in 3-dimensional projective space $\mathbb{P}^3_{\mathbb{F}_{2^n}}$) a smooth algebraic surface of a class known as *Fermat hypersurfaces*, which have been studied from the arithmetic and geometric points of view

- ☞ One we can apply the Lang-Weil estimates and conclude that the number of solutions to $Z_0^e + Z_1^e + Z_2^e + Z_3^e = 0$ (in projective 3-space, i.e., up to multiplication by a common constant) over $\mathbb{F}_{2^n}$ is $q^2 + O(q^{3/2})$ where $q := 2^n$ and the constant implied by $O(q^{3/2})$ is absolute.

Some references on bent functions :

- J. F. Dillon, " Elementary Hadamard difference sets". PhD dissertation. Univ. of Maryland, 1974.
- C. Carlet, " Boolean Functions for Cryptography and Error Correcting Codes". Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257-397, 2010.
- A. Kholosha and A. Pott, "Bent functions and related functions", Section 9.3 in the Handbook Finite fields, 2013.
- C. Carlet, "Open problems on binary bent functions", LNCS, Springer, pp. 203-241, 2014.
- C. Carlet and S. Mesnager, "Four decades of research on bent functions". Journal Designs, Codes and Cryptography (DCC), Springer (special issue, jubilee). To appear.
- S. Mesnager, Book "Bent functions : fundamentals and results", Springer, New York. (approx. 450 pages). To appear.