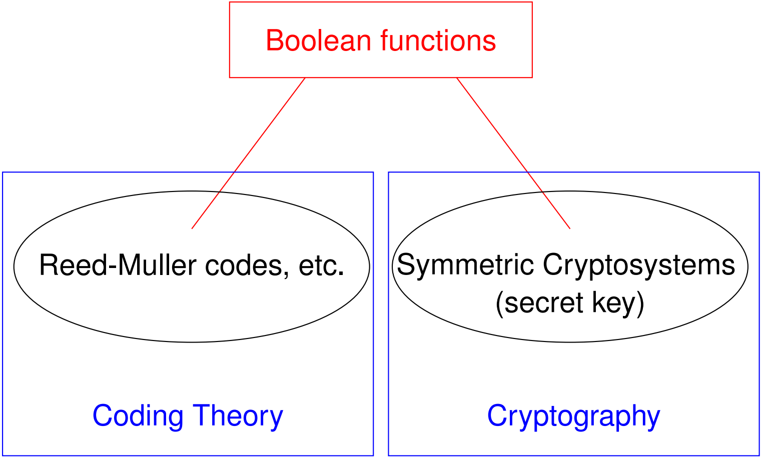
“Reader digest of " 16-year achievements on Boolean functions and open problems

Sihem Mesnager

University of Paris VIII (department of Mathematics),
University of Paris XIII (LAGA), CNRS and Telecom Paris

The 5th International Conference on Boolean functions and their Applications (BFA 2020)
15-17 September 2020, Norway

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

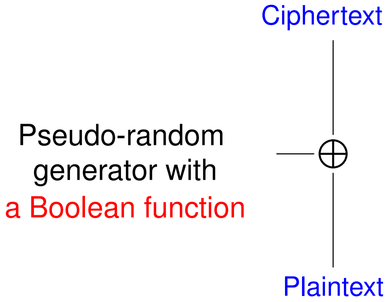


$\mathcal{B}_n = \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$

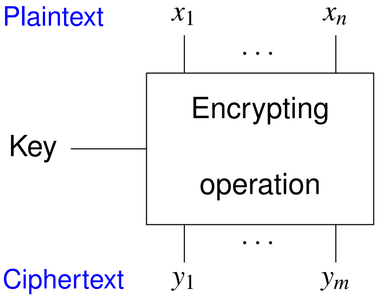
- The Reed-Muller code $\mathcal{RM}(r,n)$ can be defined in terms of **Boolean functions** : $\mathcal{RM}(r,n)$ is the set of all n-variable Boolean functions $\mathcal{B}_n$ of algebraic degrees at most r. More precisely, it is the linear code of all binary words of length 2^n corresponding in the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

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

Stream ciphers



Bloc ciphers (AES, DES, etc)

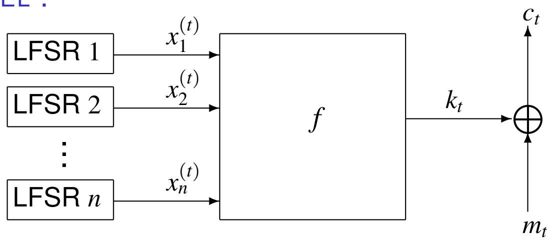


outputs of Boolean functions (depending on the key) over $x_1, \cdots, x_n$

The two models of pseudo-random generators with a Boolean function :

COMBINER MODEL :

m_t : plain text
c_t : cipher text
k_t : key stream

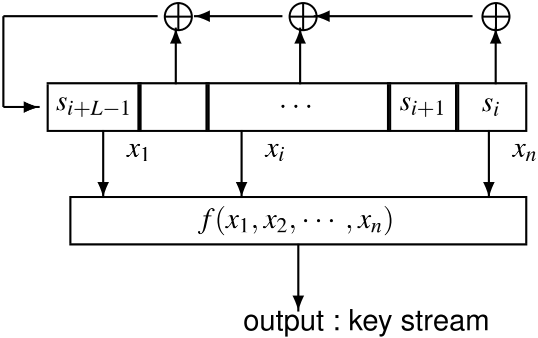


LFSR : Linear Feedback Shift Register

• A Boolean function combines the outputs of several LFSR to produce the key stream : **a combining (Boolean) function f**.

•The initial state of the LFSR's depends on a secret key.

FILTER MODEL :



- A Boolean function takes as inputs several bits of a single LFSR to produce the key stream : **a filtering (Boolean) function** f
  - ☞ 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** !

Some main cryptographic criteria for Boolean functions

- CRITERION 1 : To protect the system against distinguishing attacks, the cryptographic function must be balanced, that is, its Hamming weight is 2^{n-1}.

- CRITERION 2 : The cryptographic function must have a high algebraic degree to protect against the Berlekamp-Massey attack.

The Hamming distance $d_H(f,g) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) \neq g(x)\}$.

- CRITERION 3 : To protect the system against linear attacks and correlation attacks, the Hamming distance from the cryptographic function to all affine functions must be large.
- CRITERION 4 : To be resistant against correlation attacks on combining registers, a combining function f must be m-resilient where m is as large as possible.

Algebraic immunity of f : $\mathrm{AI}(f)$ is the lowest degree of any nonzero function g such that $f \cdot g = 0$ or $(1+f) \cdot g = 0$.

- CRITERION 5 : To be resistant against algebraic attacks, f must be of high algebraic immunity that is, close to the maximum $\lceil \frac{n}{2} \rceil$. But this condition is not sufficient because of Fast Algebraic Attacks (FFA) : cryptographic functions should be resistant against FFA !

Some of these criteria are antagonistic ! Tradeoffs between all these criteria must be found.

Definition (The discrete 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 $x \cdot y = \sum_{i=1}^n x_i y_i, \forall x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, \quad \forall y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$.

or

Definition (The discrete 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 $\mathbb{F}_{2^n}$.

Cryptographic parameters for Boolean and vectorial functions

- Nonlinearity and higher-order nonlinearity
- Correlation immunity and resiliency
- Algebraic immunity and fast algebraic immunity
- Boomerang uniformity
- etc.

Interests are in four aspects :

1. Characterizations
2. Constructions
3. Classifications
4. Enumerations

Extension of the theory of cryptographic Boolean functions to :

1. Vectorial Boolean functions
2. Functions in odd characteristic
3. Generalized functions

A much particular interest in :

- Bent Boolean functions
- Bent vectorial Boolean functions
- Subclasses of bent Boolean functions : hyper-bent Boolean functions
- Super classes of bent Boolean functions : plateaued Boolean functions

☞ Book [SM, 2016] : Bent Functions - Fundamentals and Results. Springer 2016

☞ Survey [Carlet-SM 2016] : Four decades of research on bent functions. Des. Codes Cryptogr. 2016

- Reed-Muller codes
- Minimal codes
- LRC codes
- LCD codes
- etc.

Approaches : algebraic approach, combinatoric approach, asymptotic approach and geometric approach.

Mathematical tools :

- discrete Fourier/Walsh transforms
- polynomials over finite fields (polynomials, Linearized polynomials, permutation polynomials, involutions, Dickson polynomials, polynomials e- to-1, etc)
- functions over finite fields (symmetric functions, quadratic forms, etc)
- tools from algebraic geometry (algebraic curves, elliptic curves, hyper-elliptic curves, etc)
- finite geometry (oval polynomials, hyperovals, etc)
- linear algebra and group theory
- tools from combinatorics
- tools from arithmetic number theory

Definition

An n-variable Boolean function f is said to be correlation immune of order k if any sub-function deduced from f by fixing at most k inputs is balanced, equivalently,

$$\widehat{\chi_f}(v) = 0 \text{ for all } v \in \mathbb{F}_2^n \text{ such that } 1 \le w_H(v) \le k$$

If f is moreover balanced then f is said to be resilient of order k.

- A cryptographic criterion : a (combining) Boolean function must be resilient of order m with m large.
- A new application of correlation immune functions (not resilient) in relation with block ciphers is with the counter-measure against side channel attacks.

Estimating the number of Boolean functions satisfying one or more cryptographic criteria is useful :

- it indicates for which values of parameters there is a chance of finding good cryptographic Boolean functions by random search.
- a large number of Boolean functions is necessary if we want to impose several constraints on the function.

☞ Count the number of m-resilient n-variable Boolean functions (**seems to be an intractable open problem !**)

NOTATION

✎ *Res_n^m : the set of all n-variable Boolean functions which are m-resilient.*

✎ *$\#Res_n^m$: the cardinality of Res_n^m.*

Known results for $\#Res_n^m$

- The value of $\#Res_n^m$ is known for $m \geq n-3$ [Camion et al 1991].
- The value of $\#Res_n^1$ is known for $n \leq 7$ [Harary-Palmer 1973], [Le Bars-Viola 2007].
- Asymptotic estimation on $\#Res_n^m$ [Canfield et al 2010].
- Upper bounds : [Schneider 1990] (b_1), [Carlet-Klapper 2002] (b_2), [Carlet-Gouget 2002] (b_3) :

b_1 is better than b_2 and b_3

b_2 and b_3 improve upon b_1

$b_2 \geq b_3$ $\quad$ $b_3 \geq b_2$

m

1 $\quad$ $\frac{n}{2}$ $\quad$? $\quad$ $n-3$

We use the characterization of the resiliency by means of the Numerical Normal Form (N.N.F) (representation of a Boolean function as polynomial over $\mathbb{Z}$).

DEFINITION (CARLET-GUILLOT 1999)

We call Numerical Normal Form (NNF) the representation of pseudo-Boolean functions in $\mathbb{R}[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$.

We use the characterization of the resiliency by means of the Numerical Normal Form (N.N.F) (representation of a Boolean function as polynomial over $\mathbb{Z}$).

PROPOSITION (CARLET-GUILLOT 1999)

Let $f : \mathbb{F}_2^n \to \{0,1\}$ *Let* $g(x) = f(x) \oplus x_1 \oplus \cdots \oplus x_n$ *(viewed as an integer-valued function). Then* f *is* m*-resilient if and only if,* $\deg_{NNF}(g) \leq n - m - 1$

1. We show that counting m-resilient n-variable Boolean functions is equivalent to count the number of integer points in a particular convex polytope.
2. We introduce a multivariate generating function whose one of its coefficients is $\#Res_n^m$.
3. This derives us to interpret $\#Res_n^m$ as a Taylor coefficient in the series expansion of a multivariate partial fraction.

Proposition (SM 2007)

$\#Res_n^m$ is the coefficient of $\prod_{I\subseteq\{1,\ldots,n\}} z_I^{b_{|I|}+1}$ in the series expansion of

$$\prod_{I\subseteq\{1,\ldots,n\}}(1+z_I)\prod_{\#J\leq n-m-1}\frac{1}{1-\prod_{I\supseteq J} z_I}$$

where

$$b_i=\sum_{j=1}^{\min(i,n-m-1)}\binom{i}{j}2^{j-1},\quad i\in\{0,\ldots,n\}$$

Proposition ([SM 2007])

$$\#Res_n^m=\frac{1}{(2i\pi)^{2^n}}\int\cdots\int_{\gamma\subset\mathbb{C}}\prod_{I\subseteq\{1,\ldots,n\}}\frac{1+z_I}{z_I^{b_{\#I}+2}}\prod_{\#J\leq n-m-1}\frac{1}{1-\prod_{I\supseteq J} z_I}\prod_{I\subseteq\{1,\ldots,n\}} dz_I$$

OPEN PROBLEM

Compute the value of $\#Res_n^m$ for $n > 7$ or improve the known upper bounds on $\#Res_n^m$.

A CRYPTOGRAPHIC CRITERION : The distance of a cryptographic function to all affine functions must be high to protect the system against linear attacks and correlation attacks.

- ☞ The nonlinearity of f is the minimum Hamming distance to affine functions :

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 : is the set of affine functions over $\mathbb{F}_{2^n}$.

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 : $nl_r(f) = \min_{g \in \mathcal{RM}(r,n)} d_H(f, g)$

☞ We were interested in :

- for a given integer k, $nl_r(f)$ of n-variable Boolean functions f with algebraic immunity k.
- the maximal value of $nl_r(f)$ ($r > 1$) of n-variable Boolean functions f.

- In 2005 : [Lobanov 2005] provided a lower bound on the $nl_r(f)$: $nl_r(f) \geq 2\sum_{i=0}^{k-r-1} \binom{n-r}{i}$
- In 2006 : two lower bounds on $nl_r(f)$ involving the algebraic immunity ([Carlet 2006],[Carlet-Dalai-Gupta-Maitra 2006]). None of them is better than the other one for all values of the algebraic immunity.

- In 2008 : a new lower bound on the rth-order nonlinearity profile of Boolean functions, given their algebraic immunity, that improves significantly upon the known lower bounds [Carlet et al. 2006] for all orders and upon the bound [Carlet 2006] for low orders :

THEOREM (SM 2008)

Let f be an n-variable Boolean function of algebraic immunity k and let r be a positive integer strictly less than k. Then

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$$

- In 2010 : [Rizomiliotis 2010] gave precisions on the bounds, involving the maximum between the minimal algebraic degree of the nonzero annihilators of f and the minimal algebraic degree of the nonzero annihilators of f$\oplus 1$.
- In 2015 : [SM, McGrew, Davis, Steele, Marsten 2015] constructed a family of Boolean functions where the first bound [Carlet 2006](the presumed weaker bound) is tight and the second bound [Carlet et al. 2006] is strictly worse than the first bound. They showed that the difference between the two bounds can be made arbitrarily large.
- In 2020 : [Carlet 2020] gave a very general proof of Lobanov result.

Open problem

Improve further the known lower bounds on the rth-order nonlinearity profile of Boolean functions, given their algebraic immunity.

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

- 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 $\rho(r,n)$ $(r > 1)$ before 2007 : [Cohen-Litsyn 1992].

[Carlet-SM 2007] Let $r > 1$. The covering radius of the Reed-Muller code of order r satisfies
asymptotically :$\rho(r,n) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{n/2} + O(n^{r-2})$
Our results have improved the best known upper bounds dating from 15 years ago. Up to now, our bounds are the best bounds known in the literature.
Our results are obtained by induction on r thanks to improved upper bounds on the covering radius $\rho(2,n)$:

Theorem (Carlet-SM 2007)

For every positive integer $n \geq 17$, the covering radius $\rho(2,n)$ of the second-order Reed-Muller code $\mathcal{RM}(2,n)$ is upper bounded by

$$\left\lfloor 2^{n-1} - \frac{\sqrt{15}}{2} \cdot 2^{\frac{n}{2}} \cdot \left(1 - \frac{122929}{21 \cdot 2^n} - \frac{155582504573}{4410 \cdot 2^{2n}}\right) \right\rfloor \tag{1}$$

Brief outline of the proof

$B_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$.
We prove an asymptotic upper bound on the covering radius $\rho(2, n)$ of the Reed-Muller code of order 2 :

$$\rho(2, n) \leq 2^{n-1} - \sqrt{15}\, 2^{\frac{n}{2}-1} + O(1).$$

Indeed, we have :

$$\boxed{\forall k \in \mathbb{N}, \quad \rho(2, n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}}$$

where

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}, f \in \mathcal{B}_n,\, k \in \mathbb{N}$$

Brief outline of the proof

$$\boxed{\forall k \in \mathbb{N}, \quad \rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}}$$

1. Decomposition of $\mathcal{S}_k(f)$ into sums of characters :
$S_k(f) = \sum_{w=0}^{k} N_k^{(2w)} M_f^{(2w)}$ where $M_f^{(2w)} = \sum_{\substack{g \in \mathcal{RM}(n-3,n) \\ wt(g)=2w}} (-1)^{\langle f,g \rangle}$
and $N_k^{(2w)}$ is an integer independent of f.
2. Lower bound of the sums of characters $M_f^{(2w)}$ thanks to the characterization of the words of Reed-Muller codes given by Kasami, Tokura and Azumi : $\forall f \in \mathcal{B}_n$, $M_f^{(2w)} \geq M_{min}^{(2w)}$.
3. Lower bound of $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$, $\forall f$, leading to an upper bound
$\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}}$ for $k \leq \mathrm{k}_n$ where k_n varies according to the value of n and $\mathcal{S}_k^{min} = \sum_{w=0}^{k} N_k^{(2w)} M_{min}^{(2w)}$.

Remarks :

- The greater we take the value of k, the better the upper bound obtained.
- Our method could be applied directly to $\rho(r,n)$ but the best result is obtained with our method to $\rho(2,n)$.
- We were able to improve $\rho(2,n)$ thanks to the characterization of those elements of the $\mathcal{RM}(r,n)$ whose Hamming weights are $< 2.5\ d_{min}$.

OPEN PROBLEM

Improve further the covering radius of the Reed-Muller code $\mathcal{RM}(2,n)$ by getting a better estimation of the sums of characters $M_f^{(2w)}$.

- ☞ 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.

DEFINITION (BENT FUNCTION [ROTHAUS 1976])

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

- **A main characterization of bentness :**

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

- ☞ some classes of bent functions are known (Maiorana-Mc Farland's class, Spreads class $\mathcal{PS}^-$, $\mathcal{PS}_{ap}$, Class H).

Spread

DEFINITION (SPREAD)

A m-spread of $\mathbb{F}_{2^n}$ is a set of pairwise supplementary m-dimensional subspaces of $\mathbb{F}_{2^n}$ whose union equals $\mathbb{F}_{2^n}$

EXAMPLE (A CLASSICAL EXAMPLE OF m-SPREAD)

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

☞ We were interested in bent functions g defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, whose restrictions to elements of the m-spread $\{E_a, E_\infty\}$ are linear.

Class $\mathcal{H}$

Functions g of the class $\mathcal{H}$ defined over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ whose restrictions to elements of the m-spread $\{E_a, E_\infty\}$ are linear, are of the form (2)

$$g(x,y) = \begin{cases} Tr_1^m\left(x\psi\left(\frac{y}{x}\right)\right) \text{ if } x \neq 0 \\ Tr_1^m(\mu y) \text{ if } x = 0 \end{cases} \quad (2)$$

where $\psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ et $\mu \in \mathbb{F}_{2^m}$.

THEOREM (CARLET-SM 2010)

A function g of the class $\mathcal{H}$ si bent if and only if

$$G(z) := \psi(z) + \mu z \text{ is a permuation on } \mathbb{F}_{2^m} \quad (3)$$

$$\forall \beta \in \mathbb{F}_{2^m}^\star, \text{ the function } z \mapsto G(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m}. \quad (4)$$

- the condition (4) implies condition (3).
- A function G from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ satisfying (4) if and only if for all $\gamma \in \mathbb{F}_{2^m}$, 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 over $\mathbb{F}_{2^m}$.

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
$D(f) = \{(1,t,f(t)), t \in \mathbb{F}_{2^n}\} \cup \{(0,1,0),(0,0,1)\}$ where f is an o-polynomial.

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

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

Class $\mathcal{H}$ —(1)— **Niho bent functions**

(2)

o-polynomials

Open problem

Find new Niho bent functions and find new o-polynomials.

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)

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

- Hyper-bent functions have properties stronger than bent functions ; they are rarer than bent functions.
- ☞ Hyper-bent functions are used in S-boxes (DES).
- ☞ A new criterion [Canteaut-Rotella, 2016] given on filtered LFSRs has revived the interest in hyper-bent functions.
- ☞ New results on (generalized) hyper-bent functions [SM 2020].

NOTATION

We denote by $\mathcal{D}_n$ the set of bent functions f defined on $\mathbb{F}_{2^n}$ by $f(x) = \sum_i Tr_1^{o(d_i)}(a_i x^{d_i})$ 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 $\mathcal{D}_n$.
- In 2020, [SM-Mandal-Tang, 2020] provided new construction method and characterizations of the hyper-bentness property.

OPEN PROBLEM

Find new hyper-bent functions outside the set $\mathcal{D}_n$.

Conclusions

- An intensive work has been done on Boolean functions but many interesting problems are still open.
- An important reference in this topic is the extraordinary book of Claude Carlet entitled "Boolean Functions for Cryptography and Coding Theory " to appear in Cambridge Press.

Book of Claude Carlet