

**Image sets, nonlinearity and distance to  
affine functions of  $\delta$ -uniform functions, and  
 $\gamma$ -functions of APN functions**

Claude Carlet

University of Bergen, Norway ; University of Paris 8, France

# Outline

- ▶ Known results on the image sets of differentially uniform functions
- ▶ On the nonlinearity of differentially uniform functions
- ▶ On the distance to affine functions
  - Case of differentially uniform functions
  - Upper bounds for general vectorial functions
- ▶ On the  $\gamma$ -functions associated to general APN functions
  - Linear structures of  $\gamma_F$  and bent components of  $F$
  - Relation between  $W_{\gamma_F}$  and  $W_F$ ; deduced relation on  $W_F$
  - Lower bound on the nonlinearity of a class of APN functions
  - Relation between the nonlinearities of  $F$  and  $\gamma_F$

## Known results on differentially uniform functions

[CHP 2017] “C. C., A. Heuser and S. Picek. Trade-Offs for S-Boxes : Cryptographic Properties and Side-Channel Resilience. ACNS 2017” (not very well known) :

Let  $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$  be any  $(n, m)$ -function (to be used as an S-box in a block cipher) and for  $a \in \mathbb{F}_2^n$ , define the so-called derivative of  $F$  :

$$D_a F(x) = F(x) + F(x + a).$$

$$\begin{aligned}
& \sum_{a \in \mathbb{F}_2^n; a \neq 0_n} |(D_a F)^{-1}(0_m)| = \\
& |\{(x, y) \in (\mathbb{F}_2^n)^2; F(x) = F(y)\}| - 2^n = \\
& \sum_{b \in \text{Im}(F)} |F^{-1}(b)|^2 - 2^n \geq \\
& \frac{\left(\sum_b |F^{-1}(b)|\right)^2}{|\text{Im}(F)|} - 2^n = \\
& \frac{2^{2n}}{|\text{Im}(F)|} - 2^n.
\end{aligned}$$

Hence :

$$\frac{\sum_{a \in \mathbb{F}_2^n; a \neq 0_n} |(D_a F)^{-1}(0_m)|}{2^n - 1} \geq \frac{\frac{2^{2n}}{|Im(F)|} - 2^n}{2^n - 1},$$

which implies :

$$\max_{a \in \mathbb{F}_2^n; a \neq 0_n} |D_a F^{-1}(0_m)| \geq \frac{\frac{2^{2n}}{|Im(F)|} - 2^n}{2^n - 1}.$$

The differential uniformity  $\delta_F$  of  $F$ , equal by definition to :

$$\max_{\substack{a \in \mathbb{F}_2^n, a \neq 0_n \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n; F(x) + F(x + a) = b\}| = \max_{\substack{a \in \mathbb{F}_2^n, a \neq 0_n \\ b \in \mathbb{F}_2^m}} |(D_a F)^{-1}(b)|,$$

satisfies then :

$$\delta_F \geq \left\lceil \frac{\frac{2^{2n}}{|Im(F)|} - 2^n}{2^n - 1} \right\rceil.$$

Equivalently, we have the following bound on the image set size :

$$|Im(F)| \geq \left\lceil \frac{2^{2n}}{(2^n - 1) \delta_F + 2^n} \right\rceil \geq \left\lceil \frac{2^n}{\delta_F + 1} \right\rceil.$$

For almost perfect nonlinear (APN)  $(n, n)$ -functions ( $\delta_F = 2$ ) :

$$|Im(F)| \geq \left\lceil \frac{2^{2n}}{3 \cdot 2^n - 2} \right\rceil. \quad (1)$$

Bound (1), which is tight (achieved by APN power functions in even dimension  $n$ ), has been recently rediscovered in :

[I. Czerwinski. On the minimal value set size of APN functions. IACR ePrint Archive, 2020], with  $\left\lceil \frac{2^{2n}}{3 \cdot 2^n - 2} \right\rceil = \begin{cases} \frac{2^n + 1}{3}, n \text{ odd,} \\ \frac{2^n + 2}{3}, n \text{ even} \end{cases}$ .

This proof generalizes straightforwardly to any characteristic :

$$\delta_F \geq \left\lceil \frac{\frac{p^{2n}}{|Im(F)|} - p^n}{p^n - 1} \right\rceil ,$$

which implies :

$$|Im(F)| \geq \left\lceil \frac{p^{2n}}{(p^n - 1) \delta_F + p^n} \right\rceil \geq \left\lceil \frac{p^n}{\delta_F + 1} \right\rceil ,$$

and this has been found “again” in :

[L. Kölsch, B. Kriepke and G.M. Kyureghyan. Image sets of perfectly nonlinear maps. arXiv, 2020].



# On the nonlinearity of differentially uniform functions

Recall that the *nonlinearity* of an  $(n, m)$ -function  $F$  equals the minimum Hamming distance between its component functions  $v \cdot F$ ,  $v \neq 0_m$  (where  $\cdot$  is any inner product), and affine Boolean functions  $u \cdot x + \epsilon$ .

Equivalently, using the Walsh transform of  $F$  :

$$W_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x}, \text{ we have :}$$

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{u \in \mathbb{F}_2^n \\ v \in \mathbb{F}_2^m, v \neq 0_m}} |W_F(u, v)|.$$

The covering radius bound writes :  $nl(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ , and is achieved with equality by the so-called *bent functions*, which exist if and only if  $m \leq \frac{n}{2}$ ,  $n$  even, according to K. Nyberg.

In [CHP 2017] is proved :  $nl(F) \leq 2^{n-1} - \frac{2^{n+m-1} - 2^{n-1}}{2^m - 1}$ .

This bound is weak. Let us improve it. We have :

$$\sum_{v \in \mathbb{F}_2^m} W_F^2(0_n, v) = 2^m |\{(x, y) \in \mathbb{F}_2^n; F(x) = F(y)\}| \geq \frac{2^{2n+m}}{|Im(F)|},$$

$$\text{and then : } \max_{v \in \mathbb{F}_2^m, v \neq 0_m} W_F^2(0_n, v) \geq \frac{\frac{2^{2n+m}}{|Im(F)|} - 2^{2n}}{2^m - 1},$$

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

This bound is sharper than the covering radius bound if and only if  $|Im(F)| < \frac{2^{n+m}}{2^n + 2^{m-1}}$  (which ranges from roughly  $2^m$  to  $2^{m-1}$  when  $m$  ranges from  $\frac{n}{2}$  to  $n$ ).

## On the distance to affine functions

Let  $\mathcal{A}$  denote the space of affine  $(n, m)$ -functions,  $d_H$  denote the Hamming distance and  $d_H(F, \mathcal{A}) = \min_{A \in \mathcal{A}} d_H(F, A)$ .

We have  $d_H(F, \mathcal{A}) \geq nl(F)$  as shown in :

[LMC 2017] “J. Liu, S. Mesnager and L. Chen. On the nonlinearity of S-boxes and linear codes. Cryptography and Communications, 2017” .

*For differentially uniform functions* : For every affine function  $A$ , we have :

$$d_H(F, A) = |\{x \in \mathbb{F}_2^n; F(x) + A(x) \neq 0_m\}| \geq |Im(F + A)| - 1.$$

We deduce then from the bound on the image set size :

$$d_H(F, \mathcal{A}) \geq \left\lceil \frac{2^{2n}}{(2^n - 1)\delta_F + 2^n} \right\rceil - 1, \quad (2)$$

but this bound is weak. Let us improve it. We have :

$$\begin{aligned} |F^{-1}(0_m)| &\leq \sqrt{\sum_{b \in \mathbb{F}_2^n} |F^{-1}(b)|^2} = \\ &\sqrt{|\{(x, y) \in (\mathbb{F}_2^n)^2; F(x) = F(y)\}|} = \\ &\sqrt{\sum_{a \in \mathbb{F}_2^n} |(D_a F)^{-1}(0_m)|} \leq \sqrt{2^n + \delta_F (2^n - 1)}. \end{aligned}$$

Applying this to  $F + A$  instead of  $F$ , we deduce :

$$d_H(F, A) \geq 2^n - \sqrt{2^n + \delta_F (2^n - 1)}.$$

Hence :

$$d_H(F, \mathcal{A}) \geq 2^n - \sqrt{2^n + \delta_F (2^n - 1)}.$$

In particular, for APN functions :

$$d_H(F, \mathcal{A}) \geq 2^n - \sqrt{3 \cdot 2^n - 2} \text{ (rather large).}$$

For general  $(n, m)$ -functions :

[LMC 2017] proved by using the Walsh transform :

$d_H(F, \mathcal{A}) < (1 - 2^{-m})(2^n - 1)$ . Note that this means :

$$d_H(F, \mathcal{A}) \leq \begin{cases} 2^n - 2^{n-m} - 1 & \text{for } m \leq n \\ 2^n - 2 & \text{for } m \geq n. \end{cases}$$

- Slight improvement when  $m < n$  :

For every linear  $(n, m)$ -function  $L$ , we have :

$$\max_{b \in \mathbb{F}_2^m} |\{x \in \mathbb{F}_2^n; F(x) + L(x) = b\}|^2 \geq$$

$$\frac{\sum_{b \in \mathbb{F}_2^m} |\{x \in \mathbb{F}_2^n; F(x) + L(x) = b\}|^2}{2^m} =$$

$$2^{-m} |\{(x, y) \in (\mathbb{F}_2^n)^2; F(x) + L(x) = F(y) + L(y)\}| =$$

$$2^{-2m} \sum_{x, y \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m} (-1)^{v \cdot (F(x) + F(y) + L(x+y))}.$$

We have, for  $v \neq 0_m$  that :

$$\sum_{L \in \mathcal{L}} (-1)^{v \cdot L(x+y)} = \begin{cases} |\mathcal{L}| & \text{if } x + y = 0_n \\ 0 & \text{otherwise.} \end{cases}$$



We deduce (distinguishing the cases  $v = 0_m$  and  $v \neq 0_m$ ) :

$$\sum_{L \in \mathcal{L}} \max_{b \in \mathbb{F}_2^m} |\{x \in \mathbb{F}_2^n; F(x) + L(x) = b\}|^2 \geq (2^{2n-2m} + (2^m - 1)2^{n-2m})|\mathcal{L}|.$$

This leads to :

$$d_H(F, \mathcal{A}) \leq 2^n - \left\lceil 2^{\frac{n}{2}-m} \sqrt{2^n + 2^m - 1} \right\rceil.$$

- Stronger improvement when  $m \geq n - \ln n$  :

Let  $a \in \mathbb{F}_2^n$  and let  $a_1, \dots, a_n$  be linearly independent in  $\mathbb{F}_2^n$ .

Let  $A$  be the unique affine function such that  $A(a) = F(a)$  and  $A(a + a_i) = F(a + a_i)$  for  $i = 1, \dots, n$ .

Then we have  $d_H(F, A) \leq 2^n - (n + 1)$  since  $A$  and  $F$  coincide at the  $n + 1$  distinct points  $a, a + a_1, \dots, a + a_n$ .

We have then :

$$d_H(F, \mathcal{A}) \leq 2^n - n - 1.$$

We could prove that no function exists achieving this bound as an equality.

*Question* : is it possible to further reduce the gap between the lower bound  $d_H(F, \mathcal{A}) \geq 2^n - \sqrt{3 \cdot 2^n - 2}$ , valid for  $F$  APN, and the upper bound  $d_H(F, \mathcal{A}) \leq 2^n - n - 1$ , valid for any  $(n, n)$ -function ?

## On the $\gamma$ -functions associated to general APN functions

[CCZ 1998]" C.C., P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography, 1998" :

given  $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ , the Boolean function :

$$\gamma_F(a, b) = \begin{cases} 1 & \text{if } a \neq 0 \text{ and } \{x \in \mathbb{F}_2^n; F(x) + F(x + a) = b\} \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

is bent if and only if  $F$  is almost bent (i.e.  $F$  has nonlinearity  $2^{n-1} - 2^{\frac{n-1}{2}}$ ;  $n$  must then be odd).

For general APN functions, the only known results are that :

-  $\gamma_F$  has weight  $2^{2n-1} - 2^{n-1}$  ; more precisely,  $b \mapsto \gamma_F(a, b)$  is

balanced for  $a \neq 0_n$  and null for  $a = 0_n$ ,

-  $\sum_{b \in \mathbb{F}_2^n} b \gamma_F(a, b) = \sum_{x \in \mathbb{F}_2^n} F(x)$ , for every  $a \neq 0_n$ ,

-  $\forall a \neq 0_n, b, a' \neq 0_n, a \neq a' :$

$(\gamma_F(a, b) = 1) \Rightarrow (\exists b'; \gamma_F(a', b') = \gamma_F(a + a', b + b') = 1),$

- For every  $u, v \in \mathbb{F}_2^n$  :

$$W_{\gamma_F}(u, v) = \sum_{a, b \in \mathbb{F}_2^n} (-1)^{\gamma_F(a, b) + u \cdot a + v \cdot b} = \begin{cases} 2^n & \text{if } v = 0_n, \\ 2^n - W_F^2(u, v) & \text{if } v \neq 0_n. \end{cases}$$

*Linear structures of  $\gamma_F$  and bent components of  $F$  :*

We shall say that  $(\alpha, \beta)$  is an  $\epsilon$ -valued linear structure of  $F$  if :

$$D_{(\alpha, \beta)}\gamma_F(a, b) = \gamma_F(a, b) + \gamma_F(a + \alpha, b + \beta) \equiv \epsilon.$$

Characterization by the Walsh transform :

$$\forall u, v \in \mathbb{F}_2^n, (\alpha \cdot u + \beta \cdot v = \epsilon + 1) \Rightarrow W_{\gamma_F}(u, v) = 0.$$

Function  $\gamma_F$  admits then :

- no 1-valued linear structure,
- no linear structure  $(\alpha, \beta)$  such that  $\alpha \neq 0_n$ .

For  $\beta \in \mathbb{F}_2^n$ ,  $(0_n, \beta)$  is a 0-valued linear structure of  $\gamma_F$  if and only if  $v \cdot F$  is bent for every  $v \notin \{0_n, \beta\}^\perp$  (i.e. we have an affine hyperplane of bent components of  $F$ ). So,  $n$  must then be even.

Open : for  $n$  even, determine if  $\gamma_F$  can have linear structures.

*Negative results* : for every APN power  $(n, n)$ -function  $F$ , the  $\gamma_F$  function has no (nonzero) linear structure. A super-class of almost bent functions has the same inexistence property.

Other open questions :

- Maximum dimension of affine spaces of bent components ?
- Maximum dimension of affine spaces of bent Boolean functions ?

The maximum number of bent components is known :  $2^n - 2^{\frac{n}{2}}$  :

[PMB 2018] "A. Pott, E. Pasalic, A. Muratović-Ribić and S. Bajrić. On the Maximum Number of Bent Components of Vectorial Functions. *IEEE Transactions on Information Theory*, 2018."

*More on bent components :*

- For every  $v \neq 0_n$ ,  $v \cdot F$  is bent if and only if, for every  $a \in \mathbb{F}_2^n$ , the Boolean function  $b \mapsto \gamma_F(a, b) + v \cdot b$  is balanced.
- $F$  has  $2^n - 2^{\frac{n}{2}}$  bent components if and only if there exists an  $\frac{n}{2}$ -dimensional vector subspace  $V$  of  $\mathbb{F}_2^n$  such that any pair  $(0_n, \beta)$  with  $\beta \in V$  is a 0-valued linear structure of  $\gamma_F$ .

Hence, APN power functions cannot have  $2^n - 2^{\frac{n}{2}}$  bent components.

This result is complementary with that of : [MZZT 2019] “S. Mesnager, F. Zhang, C. Tang and Y. Zhou. Further study on the maximum number of bent components of vectorial functions. Designs, Codes and Cryptography, 2019”, which shows the same for plateaued APN functions.



*A property on  $W_F$  deduced from a relation on  $W_{\gamma_F}$  :*

The Titsworth relation applied to  $\gamma_F$  writes :

$$\forall (u_0, v_0) \neq (0_n, 0_n), \sum_{u, v \in \mathbb{F}_2^n} W_{\gamma_F}(u, v) W_{\gamma_F}(u + u_0, v + v_0) = 0.$$

It implies that, for every  $(u_0, v_0)$  and every APN  $(n, n)$ -function  $F$  :

$$\sum_{\substack{u, v \in \mathbb{F}_2^n \\ v \neq 0_n, v \neq v_0}} W_F^2(u, v) W_F^2(u + u_0, v + v_0) = 2^{4n} - 2^{3n+1} + 2^{4n} \delta_0(u_0, v_0),$$

where  $\delta_0$  is the Dirac (Kronecker) symbol.

This relation looks like the known characterizations of differentially uniform functions by the Walsh transform, but is in fact different.

*Lower bound on the nonlinearity of a class of APN functions :*

If  $\{|W_F(u, v)|; u, v \in \mathbb{F}_2^n, v \neq 0_n\}$  takes its maximum for at least two different inputs  $(u, v)$ , then we have :

$$nl(F) \geq 2^{n-1} - \frac{1}{2} \sqrt[4]{2^{4n-1} - 2^{3n}}.$$

Stronger than  $nl(F) > 0$ .

All known APN functions (all are equivalent to power functions or to quadratic functions except one) satisfy the condition.

Open : Determine whether all APN functions satisfy the condition.

*Relation between the nonlinearities of  $F$  and  $\gamma_F$  :*

$$nl(\gamma_F) = 2^{n+1}nl(F) - 2(nl(F))^2 + 2^{n-1}.$$

## Conclusion

- Differentially uniform functions have large image sets.

The larger the image set, the larger the upper bound on  $nl(F)$ .

- Differentially uniform functions lie at large Hamming distance from affine functions, which preserves them from attacks based on affine approximation.

The largest possible distance to affine functions is unknown for diff. uniform functions and for general functions.

- The existence of linear structures of  $\gamma_F$  is related to that of affine spaces of bent Boolean functions.

The nonlinearities of  $F$  and  $\gamma_F$  are directly linked.

Little is known on the nonlinearity of APN (and more general diff. uniform) functions.

In particular, we do not know if they can have low nonlinearity.

A lower bound gives a beginning of explanation why the nonlinearity of all known APN functions is rather good.

We leave many open problems :

- on the existence of linear structures of  $\gamma_F$  functions for  $n$  even,
- on the largest dimension of affine spaces of bent components,
- on the largest dimension of affine spaces of bent Boolean functions.

And open questions :

- Do all APN functions take their maximum absolute Walsh value more than once?
- What are the possible values of  $nl(F)$  and  $nl(\gamma_F)$  when  $F$  is APN?

















## *References :*

C.C. Bounds on the nonlinearity of differentially uniform functions by means of their image set size, and on their distance to affine functions. IACR ePrint Archive 2020/1529. Submitted.

C.C. On the properties of the Boolean functions associated to the differential spectrum of general APN functions and their consequences. IACR ePrint Archive 2020/1587. Submitted.

# BOOLEAN FUNCTIONS *for* CRYPTOGRAPHY *and* CODING THEORY

Claude Carlet

$x_1$	$x_2$	$x_3$				
0	0	0		+		+
0	0	1		-		+
0	1	0		+		-
0	1	1		-		-
1	0	0		+		+
1	0	1		+		+
1	1	0		+		-
1	1	1		-		-