Group actions based perfect nonlinearity

Laurent Poinsot, Sami Harari

Group Actions based Perfect Nonlinearity

Laurent Poinsot and Sami Harari

Institut des Sciences de l'Ingénieur de Toulon et du Var
Université du Sud Toulon-Var
Laboratoire S.I.S.
Avenue G. Pompidou
BP 56
83162 La Valette du Var cédex, France
{poinsot,harari}@univ-tln.fr

Abstract. In a recent paper [8], we generalized the notion of perfect nonlinearity of boolean functions by replacing the translations of a vector space on $\mathbb{F}_2$ by an Abelian group of fixed-point free involutions acting regularly on this vector space. We now show this generalization to be still valid when considering a finite nonempty set X rather than a vector space on $\mathbb{F}_2$ and a faithful or regular action of a finite Abelian group G on X. We also develop a dual characterization of this new concept through the Fourier transform as for the classical notion of perfect nonlinearity. By considering faithful actions we highlight a fundamental concept underlying to perfect nonlinearity that extends the classical notions. In short we integrate the traditional concepts within a more general and primitive framework.

1 Introduction

Bent functions are those functions from $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$ such that for every nonzero $\beta \in \mathbb{F}_2^n$ the discrete Fourier transform of the $\{\pm 1\}$-valued functions $x \mapsto (-1)^{\beta \cdot f(x)}$, where the symbol "$\cdot$" denotes the usual inner product in $\mathbb{F}_2^n$, has a constant magnitude $2^{\frac{m}{2}}$. An equivalent characterization of bentness is the fact that f is perfect nonlinear or, in other terms, for every nonzero $\alpha \in \mathbb{F}_2^m$, the function $d_\alpha f : x \mapsto f(x \oplus \alpha) \oplus f(x)$ ("$\oplus$" denoting at the same time the laws of $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$), called derivative of f in direction α, takes each values equally often. Such functions have a relevant cryptographic interest that we do not recall here (see [1] and [6]).

In [8], by the substitution of the derivatives $d_\alpha f$ by functions $D_\sigma f : x \mapsto f(\sigma(x)) \oplus f(x)$, where σ is a fixed-point free involution (for all x, $\sigma(x) \neq x$ and $\sigma^2(x) = \sigma \circ \sigma(x) = x$), we generalized the traditional notion of perfect nonlinearity. More precisely we considered a kind of Abelian groups of permutations of $\mathbb{F}_2^m$ called *maximal groups of involutions*. G is such a group if $|G| = 2^m$ and every nonidentity element of G is a fixed-point free involution of $\mathbb{F}_2^m$. In this context a function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ is called *G-perfect nonlinear* if for every nonidentity $\sigma \in G$, $D_\sigma f$ is balanced. As in the classical case, the Fourier transform

leads to a dual characterization that is for every $x \in \mathbb{F}_2^m$ and every nonzero $\beta \in \mathbb{F}_2^n$, the Fourier transform of the function $\sigma \mapsto (-1)^{\beta \cdot f(\sigma(x))}$ from G to $\{\pm 1\}$ has constant magnitude $2^{\frac{m}{2}}$.

A crucial point concerning the definition of G-perfect nonlinear functions is the fact that the maximal group of involutions G acts regularly on $\mathbb{F}_2^m$(*i.e.* $\forall (x,y) \in (\mathbb{F}_2^m)^2$ there exists one and only one $\sigma \in G$ such that $\sigma(x) = y$). Then a natural way to generalize this concept is the following. Let (G, H_1, H_2) be a triple of finite Abelian groups such that G acts **faithfully** (*i.e.* the action is injective) or **regularly** (*i.e.* the action is faithful and transitive) on H_1. A function $f : H_1 \longrightarrow H_2$ is said to be G-perfect nonlinear if

$$\forall \sigma \in G \setminus \{e_G\}, \forall \beta \in H_2, |\{x \in H_1 | f(\phi(\sigma)(x)) - f(x) = \beta\}| = \frac{|H_1|}{|H_2|}$$

where e_G is neutral element of G, ϕ is the action of G on H_1 and "$f(\phi(\sigma)(x)) - f(x)$" is an abbreviation for "$f(\phi(\sigma)(x)) + (-f(x))$" where $-y$ is the inverse of y in H_2 and "$+$" the law of H_2.
If the action is regular we obtain a strict generalization of classic perfect nonlinearity. In particular the construction of G-perfect nonlinear function is than hard as within the traditional framework. However if we consider faithful actions, the constraints to define G-perfect nonlinearity are less strong than in the usual case, which implies that we have a more relevant and gradual measure of group actions perfect nonlinearity. Moreover the Fourier-transform based dual characterization of this new property is completely studied in this paper.

1.1 Our Contributions

We generalize the notion of perfect nonlinearity according to faithful or regular group actions on the input set H_1 of functions as it is described above. Furthermore we also consider regular group actions on the set of outputs H_2. Formally $f(\phi(\sigma)(x)) - f(x) = \beta$ is equivalent to $f(\phi(\sigma)(x)) = \beta + f(x) = \tau(\beta)(f(x))$ where τ is the action of H_2 on itself by translation (or by addition / multiplication depending on the notation used for the group). In our generalization we replace the action by translations by any regular group action on H_2 as it is done for the input set H_1. The dual version in terms of discrete Fourier transform is determined in a way similar to the traditional framework. For the specific case of binary G-perfect nonlinear functions, a characterization is given by the use of the new concept of G-difference sets comparable to the usual difference sets.

1.2 Organization of the Paper

In the next section some basic definitions and notations on perfect nonlinearity and group actions used in the sequel are given. The concept of perfect nonlinearity is then generalized in the context of faithful and then regular group actions on the input set of functions in Sect. 3. In the same section the existence of functions satisfying such generalized nonlinear property is proved in a constructive way. In Sect. 4 we add a regular group action on the set of outputs of functions

and show the equivalence with the previous case. In the last section G-perfect nonlinearity is totally characterized via the novel notion of G-difference sets.

2 Notations and Preliminaries

In this part are recalled some basics on bent functions and group actions. In the sequel we use the convenient abbreviation "*f.A.g.*" for "*finite Abelian group(s)*".

2.1 Dual Group, (discrete) Fourier Transform and Bent Functions

The definitions and results of this paragraph come from [2] and [5].
Let G be a *f.A.g.*. We denote by e_G its neutral element and by E its exponent *i.e.* the maximum order of its elements. A *character* of G is any homomorphism from G to the multiplicative group of E^{th} roots of unity. The set of all characters $\widehat{G}$ is an *f.A.g.*, called the *dual group of* G, isomorphic to G. We fix some isomorphism from G to $\widehat{G}$ and we denote by χ_G^α the image of $\alpha \in G$ by this isomorphism. Then $\chi_G^{e_G}$ is the trivial character *i.e.* $\chi_G^{e_G}(x) = 1\ \forall x \in G$. For instance if $G = \mathbb{F}_2^m$, $\chi_{\mathbb{F}_2^m}^\alpha : x \in \mathbb{F}_2^m \mapsto (-1)^{\alpha \cdot x}$. Until the end of this paper, any time we refer to a *f.A.g.*, we suppose that such an isomorphism has been fixed.
The *Fourier transform* of any complex-valued function f on G is defined by

$$\widehat{f}(\alpha) = \sum_{x \in G} f(x)\chi_G^\alpha(x) \text{ for } \alpha \in G.$$

We have the following and important lemma for the Fourier transform.

Lemma 1. *Let* $f : G \longrightarrow \mathbb{C}$.

1. $f(x) = 0$ *for every* $x \neq e_G$ *in* G *if and only if* $\widehat{f}$ *is constant.*
2. $\widehat{f}(\alpha) = 0$ *for every* $\alpha \neq e_G$ *in* G *if and only if* f *is constant.*

Let us introduce some notions needed to define the concept of bent functions. Let G_1 and G_2 be two *f.A.g.*. Let $f : G_1 \longrightarrow G_2$. f is said *balanced* if $\forall \beta \in G_2$, $|\{x \in G_1 | f(x) = \beta\}| = \frac{|G_1|}{|G_2|}$.
The *derivative of* f *in direction* $\alpha \in G_1$ is defined by

$$d_\alpha f : x \in G_1 \mapsto f(\alpha + x) - f(x) \in G_2 \tag{1}$$

where "$+$" is the symbol for the law of G_1 and "$y - z$" is an abbreviation for "$y * z^{-1}$" with $(y, z) \in G_2^2$, $*$ the law of G_2 and z^{-1} the inverse of z in G_2.
The function f is said *perfect nonlinear* if

$$\forall \alpha \in G_1 \setminus \{e_{G_1}\}, \forall \beta \in G_2, |\{x \in G_1 | d_\alpha f(x) = \beta\}| = \frac{|G_1|}{|G_2|}\ . \tag{2}$$

Then f is perfect nonlinear if and only if for all $\alpha \in G_1 \setminus \{e_{G_1}\}$, $d_\alpha f$ is balanced.

Proposition 1. *Let* f *be any function from* G_1 *to* G_2. *Then* f *is balanced if and only if, for every* $\beta \in G_2 \setminus \{e_{G_2}\}$, *we have*

$$\widehat{\chi_{G_2}^\beta \circ f}(e_{G_1}) = 0\ . \tag{3}$$

We can recall the notion of (generalized) bent functions. f is *generalized bent* if $\forall \alpha \in G_1$, $\forall \beta \in G_2 \setminus \{e_{G_2}\}$, $|\widehat{\chi^{\beta}_{G_2} \circ f}(\alpha)| = \sqrt{|G_1|}$ where $|z|$ is the norm for $z \in \mathbb{C}$.
Finally we have the following theorem due to Nyberg [7].

Theorem 1. *$f : G_1 \longrightarrow G_2$ is perfect non-linear if and only if it is generalized bent.*

In this paper we refer to these notions as *original*, *classical* or *traditional*, as it has been already done, so as to differentiate them from ours which are qualified as *new*, *extended* or *generalized*.

2.2 Group Action

Let G be a *f.A.g.* and X a nonempty set. $S(X)$ is the symmetric group of X. A function $\phi : G \longrightarrow S(X)$ is an action of G on X if it is a group homomorphism. In the sequel for $(\sigma, \tau) \in G^2$ and $x \in X$, we denote respectively $\phi(\sigma)(x)$ and $(\phi(\sigma) \circ \phi(\tau))(x)$ by respectively $\sigma.x$ and $\sigma \circ \tau.x$ (where "$\circ$" denotes the composition of functions). In other terms we identify $\phi(G)$ and G.
For $x \in X$, we define the *orbit* of x under the action of G by

$$\mathcal{O}_G(x) = \{\sigma.x \in X | \sigma \in G\} \ . \tag{4}$$

Let $x \in X$. The function $\phi_x : G \longrightarrow \mathcal{O}_G(x)$ such that $\phi_x(\sigma) = \sigma.x$ is called the *orbital function* of x.
An action ϕ is said *transitive* if there exists only one orbit *i.e.* for every $x \in X$, $X = \mathcal{O}_G(x)$. In other terms, $\forall (x, y) \in X^2$ there exists $\sigma \in G$ such that $\sigma.x = y$.
An injective action ϕ is called *faithful*. Note that for any action $\phi : G \longrightarrow S(X)$, $\tilde{\phi} : G/Ker\phi \longrightarrow S(X)$ such that $\tilde{\phi}(\bar{\sigma}) = \phi(\sigma)$ (where $\bar{\sigma}$ is the left coset $\sigma Ker\phi$) is a faithful action. Without loss of generality we can always suppose group actions to be at least faithful.
An action $\phi : G \longrightarrow S(X)$ is *regular* if for each $x \in X$ the orbital function $\phi_x : G \longrightarrow X$ is bijective. Indeed a regular action is a faithful and transitive action. Equivalently an action is regular if $\forall (x, y) \in X^2$ there exists one and only one $\sigma \in G$ such that $\sigma.x = y$. Note that in this case $|G| = |X|$ ($|E|$ is the cardinality of a finite set E).
The following result show the comfort to work with regular actions.

Lemma 2. *Suppose that a group G acts regularly on X. Let $(x_0, \sigma, \tau) \in X \times G \times G$. Then*

$$\sigma = \tau \Leftrightarrow \sigma.x_0 = \tau.x_0 \ .$$

Proof. The direct implication is obvious. Concerning the other implication, let $y_0 = \sigma.x_0$. Since the action is regular there exists one and only one $\pi \in G$ that maps x_0 to y_0. As σ and τ satisfy to this condition then $\sigma = \tau$. □

3 Input Group Actions based Perfect Nonlinearity

In this section we introduce the new notion of perfect nonlinearity. For functions from a *f.A.g.* H_1 to another *f.A.g.* H_2, we replace the action of H_1 on itself by translation by the action of a third *f.A.g.* G on a finite nonempty set X. In a first time we suppose the action to be only faithful which gives a finner measure of nonlinearity and later we consider regular actions. In the two contexts we establish dual notions by Fourier analysis similar to the traditional works. Finally we construct a perfect nonlinear functions in the sense of our extended definition.

3.1 Generalized Perfect Nonlinearity

Let (G, X, H) be a triple in which G and H are two *f.A.g.* such that G acts (at least) **faithfully** on the finite nonempty set X.
The *derivative* of $f : X \longrightarrow H$ in the direction $\sigma \in G$ is the function

$$D_\sigma f : x \in X \longrightarrow f(\sigma.x) - f(x) \in H \ . \tag{5}$$

where "$y_1 - y_2$" means "$y_1 + (-y_2)$" in H.
This notion is a direct generalization of the usual derivative where the action by translation is substituted by a faithful action on the inputs of a function. Using this kind of derivative we can introduce the new version of perfect nonlinearity.

Definition 1. A function $f : X \longrightarrow H$ is *G-perfect nonlinear* if for every $\sigma \in G \setminus \{e_G\}$, $D_\sigma f$ is balanced.

The definition above is valid since the action is faithful.
This approach allows us to describe new objects by playing on the "non regularity" of the action considered. Indeed the faithful property is less strong than the regularity. So by releasing these constraints, the nonlinear measuring accuracy or granularity is increased and we can describe perfect nonlinear functions from X to H by respect to a group G which can vary from the simplest form of a two-elements group to the most complex which is a group acting regularly on X.

Example 1. Let p be prime, $H = \mathbb{F}_{p^m}$ and $G = Gal(\mathbb{F}_{p^m}/\mathbb{F}_p)$ the group of Galois automorphisms of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ *i.e.* the group generated by Frobenius automorphism $\phi : x \in \mathbb{F}_{p^m} \longrightarrow x^p \in \mathbb{F}_{p^m}$. Thus G is the cyclic group of order m, $\{\phi^i | 0 \leq i \leq m-1\}$ with $\phi^i(x) = x^{p^i}$. A function $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^n}$ is G-perfect nonlinear if for each i such that $1 \leq i \leq m-1$ and for each $\beta \in \mathbb{F}_{p^m}$

$$|\{x \in \mathbb{F}_{p^m} | f(x^{p^i}) - f(x) = \beta|\} = p^{m-n}.$$

In order to illustrate the existence of such functions we now present numerical results. Let $p = 2$, $m = 8$ and $n = 1$. Let $f : x \in \mathbb{F}_{2^8} \longrightarrow x^{-1} \in \mathbb{F}_{2^8}$ (with $0^{-1} = 0$). This function occurs in AES [3] (up to the composition with an affine transformation) under the name S_{RD}. For $x \in \mathbb{F}_{2^8}$, we denote by $[x] \in \mathbb{F}_2^8$

the byte corresponding to the usual radix-two representation of x (considered as an integer modulo $2^8 = 256$) where the high-order bit is on the right and for $j = 1, \ldots, 8$, $[x]_j$ the j^{th} coordinate of $[x]$. Finally we consider for each $j \in \{1, \ldots, 8\}$, $f_j : \mathbb{F}_{2^8} \longrightarrow \mathbb{F}_2$ such that $f_j(x) = [f(x)]_j$. Then numerical computations give the following results.
For each $j \in \{1, \ldots, 8\}$ such that $j \neq 7$, f_j is $Gal(\mathbb{F}_{2^8}/\mathbb{F}_2)$-perfect nonlinear. And we have

$$|\{x \in \mathbb{F}_{2^8} | f_7(x^{2^i}) \oplus f_7(x) = 0\}| = \begin{cases} 128 \text{ if } i \neq 4, \\ 256 \text{ otherwise.} \end{cases}$$

None of these functions being perfect nonlinear in the traditional sense.

Example 2. Let H be a *f.A.g.* such that $|H| \geq 4$ and $|H| \equiv 0 \pmod 4$. Let $\sigma \in S(H)$ be a fixed-point free involution and $G = \{Id_H, \sigma\}$ the (Abelian) group generated by σ where Id_H denotes the identity function of H. Since $\forall x \in H$, $\sigma(x) \neq x$, the action of G on H is faithful. The orbits under the action of G have the form $\{x, \sigma(x)\}$ and constitute a partition of H in subsets of cardinality two. Let $I \subset G$ such that I contains exactly one and only one element of each orbit. So in particular $|I| = \frac{|G|}{2}$. By hypothesis on H, $|I|$ is an even number so we can choose a partition of I in two subsets I_1 and I_2 such that $|I_1| = |I_2| = \frac{|H|}{4}$. We define $\sigma I_k = \{\sigma(x) \in G | x \in I_k\}$ for $k = 1, 2$. We can easily check that $\{I_1, I_2, \sigma I_1, \sigma I_2\}$ is a partition of G with $|I_k| = |\sigma I_k| = \frac{|H|}{4}$ for $k = 1, 2$. Let $b \in \mathbb{F}_2$ and $f : H \longrightarrow \mathbb{F}_2$ such that $\forall x \in I_1$, $f(x) = f(\sigma(x)) = b$ and $\forall x \in I_2$, $f(x) = b$ and $f(\sigma(x)) = 1 \oplus b$. Then we have

1. $|\{x \in G | f(\sigma(x)) \oplus f(x) = 0\}| = |I_1| + |\sigma I_1| = \frac{|G|}{2}$,
2. $|\{x \in G | f(\sigma(x)) \oplus f(x) = 1\}| = |I_2| + |\sigma I_2| = \frac{|G|}{2}$.

So f is G-perfect nonlinear.

Note that if $H = \mathbb{F}_2^m$ with an odd $m > 2$, perfect nonlinear functions do not exist which is not inevitably the case for G-perfect nonlinearity as our previous example seems to indicate it. Thus we should be able to approximate in a certain way perfect nonlinearity by playing on the cardinality of G. In this sense our concept is finer than the traditional one.

The main idea in the sequel is to transform this combinatorial property in a law of "energy conservation" using Fourier techniques.

3.2 Dual Characterization with a Faithful Action on Inputs

In this subsection, we suppose that the finite nonempty set X is equipped with a finite Abelian group structure since we will consider the Fourier transform of a function defined on X (and thus we implicitly consider the dual group of X). Let (G, H_1, H_2) be a triple of *f.A.g.* such that G acts faithfully on H_1.

We introduce a binary map that should be seen as a convolutional product. Let f and g be two functions from $H_1 \longrightarrow \mathbb{C}$. We define

$$\begin{aligned} f \boxtimes g : G &\longrightarrow \mathbb{C} \\ \sigma &\mapsto (f \boxtimes g)(\sigma) = \sum_{x \in H_1} \overline{f(x)} g(\sigma.x) \end{aligned}$$

where $\bar{z}$ is the conjugate of a complex number z.
Let us compute its Fourier transform. Let $\sigma \in G$.

$$\begin{aligned} \widehat{f \boxtimes g}(\sigma) &= \sum_{\tau \in G} (f \boxtimes g)(\tau) \chi_G^\sigma(\tau) \\ &= \sum_{\tau \in G} \sum_{x \in H_1} \overline{f(x)} g(\tau.x) \chi_G^\sigma(\tau) \\ &= \sum_{x \in H_1} \overline{f(x)} \sum_{\tau \in G} g(\tau.x) \chi_G^\sigma(\tau) \ . \end{aligned} \tag{6}$$

The sum "$\sum_{\tau \in G} g(\tau.x)\chi_G^\sigma(\tau)$" satisfies the following property for each $\pi \in G$.

$$\sum_{\tau \in G} g(\tau.x)\chi_G^\sigma(\tau) = \sum_{\tau \in G} g(\tau \circ \pi.x)\chi_G^\sigma(\tau \circ \pi) = \sum_{\tau \in G} g(\tau \circ \pi.x)\chi_G^\sigma(\tau)\chi_G^\sigma(\pi) \ .$$

Then for every $\pi \in G$ we obtain

$$\begin{aligned} (6) &= \sum_{x \in H_1} \overline{f(x)} \chi_G^\sigma(\pi) \sum_{\tau \in G} g(\tau \circ \pi.x) \chi_G^\sigma(\tau) \\ &= \sum_{y \in H_1} \overline{f(\pi^{-1}.y)} \chi_G^\sigma(\pi) \sum_{\tau \in G} g(\tau.y) \chi_G^\sigma(\tau) \\ &= \sum_{y \in H_1} \overline{f(\pi^{-1}.y)} \chi_G^\sigma(\pi) \widehat{g_y}(\sigma) \end{aligned}$$

where $g_y : G \longrightarrow \mathbb{C}$ such that $g_y(\sigma) = g(\sigma.y)$.
The substitution of π by π^{-1} and the summation over G give

$$\begin{aligned} \sum_{\pi \in G} \widehat{f \boxtimes g}(\sigma) &= |G| \widehat{f \boxtimes g}(\sigma) \\ &= \sum_{x \in H_1} \sum_{\pi \in G} \overline{f(\pi.x)} \chi_G^\sigma(\pi^{-1}) \widehat{g_x}(\sigma) \\ &= \sum_{x \in H_1} \sum_{\pi \in G} \overline{f(\pi.x) \chi_G^\sigma(\pi)} \widehat{g_x}(\sigma) \\ &= \sum_{x \in H_1} \overline{\widehat{f_x}(\sigma)} \widehat{g_x}(\sigma). \end{aligned}$$

And finally we obtain a kind of trivialization of our convolutional-like product

$$\forall \sigma \in G, \ \widehat{f \boxtimes g}(\sigma) = \frac{1}{|G|} \sum_{x \in H_1} \overline{\widehat{f_x}(\sigma)} \widehat{g_x}(\sigma) \ . \tag{7}$$

Now we use this formula in the following proposition.

Proposition 2. *Let G be a f.A.g. acting faithfully on a f.A.g. H_1. Let H_2 be a f.A.g.. Let $f : H_1 \longrightarrow H_2$, $\beta \in H_2$ and $F_{\beta,f} : G \longrightarrow \mathbb{C}$ such that $F_{\beta,f}(\sigma) = \widehat{\chi^{\beta}_{H_2} \circ D_\sigma f(e_H)}$. Then we have*

$$\forall \sigma \in G,\ \widehat{F_{\beta,f}}(\sigma) = \frac{1}{|G|} \sum_{x \in H_1} |\widehat{\chi^{\beta}_{H_2} \circ f_x}(\sigma)|^2.$$

Proof. Let us compute the Fourier transform of $F_{\beta,f}$.

$$\begin{aligned}
\widehat{F_{\beta,f}}(\sigma) &= \sum_{\tau \in G} F_{\beta,f}(\tau)\chi^{\sigma}_{G}(\tau) \\
&= \sum_{\tau \in G} \sum_{x \in H_1} (\chi^{\beta}_{H_2} \circ D_\sigma f)(x)\chi^{\sigma}_{G}(\tau) \\
&= \sum_{\tau \in G} \sum_{x \in H_1} \chi^{\beta}_{H_2}(f(\tau.x) - f(x))\chi^{\sigma}_{G}(\tau) \\
&= \sum_{\tau \in G} \sum_{x \in H_1} \overline{(\chi^{\beta}_{H_2} \circ f)(x)}(\chi^{\beta}_{H_2} \circ f)(\tau.x)\chi^{\sigma}_{G}(\tau) \\
&= \sum_{\tau \in G} (\chi^{\beta}_{H_2} \circ f \boxtimes \chi^{\beta}_{H_2} \circ f)(\tau)\chi^{\sigma}_{G}(\tau) \\
&= (\widehat{\chi^{\beta}_{H_2} \circ f \boxtimes \chi^{\beta}_{H_2} \circ f})(\sigma) \\
&= \frac{1}{|G|} \sum_{x \in H_1} \overline{(\widehat{\chi^{\beta}_{H_2} \circ f})_x(\sigma)}(\widehat{\chi^{\beta}_{H_2} \circ f})_x(\sigma) \text{ (according to (7))} \\
&= \frac{1}{|G|} \sum_{x \in H_1} |(\widehat{\chi^{\beta}_{H_2} \circ f})_x(\sigma)|^2 \\
&= \frac{1}{|G|} \sum_{x \in H_1} |\widehat{\chi^{\beta}_{H_2} \circ f_x}(\sigma)|^2.
\end{aligned}$$

□

The following theorem is one of the most important result that allows us to use the Fourier transform to identify G-perfect nonlinear functions.

Theorem 2. *Let (G, H_1, H_2) be a triple of f.A.g. such that G acts faithfully on H_1. Let $f : H_1 \longrightarrow H_2$. f is G-perfect nonlinear if and only if $\forall \sigma \in G$, $\forall \beta \in H_2 \setminus \{e_{H_2}\}$,*

$$\sum_{x \in H_1} |\widehat{\chi^{\beta}_{H_2} \circ f_x}(\sigma)|^2 = |G||H_1| \ .$$

Proof. f is G-perfect nonlinear $\Leftrightarrow \forall \sigma \in G \setminus \{e_G\}$, $D_\sigma f$ is balanced over H_1
$\Leftrightarrow \forall \sigma \in G \setminus \{e_G\}$, $\forall \beta \in H_2 \setminus \{e_{H_2}\}$, $\widehat{\chi^{\beta}_{H_2} \circ D_\sigma f(e_{H_1})} = 0$ (by *proposition* 1)

$\Leftrightarrow \forall \beta \in H_2 \setminus \{e_{H_2}\}, \forall \sigma \in G \setminus \{e_G\}, F_{\beta,f}(\sigma) = 0$
$\Leftrightarrow \forall \beta \in H_2 \setminus \{e_{H_2}\}, \widehat{F_{\beta,f}}$ is constant over G (according to *lemma* 1).
By Parseval equation we obtain $\frac{1}{|G|} \sum_{\sigma \in G} |\widehat{F_{\beta,f}}(\sigma)|^2 = \sum_{\sigma \in G} |F_{\beta,f}(\sigma)|^2 = |F_{\beta,f}(e_G)|^2$.
Thus since $\widehat{F_{\beta,f}}$ is constant, $|\widehat{F_{\beta,f}}(\sigma)|^2 = |F_{\beta,f}(e_G)|^2$ for all $\sigma \in G$. Moreover $F_{\beta,f}(e_G) = \widehat{\chi^{\beta}_{H_2} \circ D_{e_G} f}(e_{H_1}) = \sum_{x \in H_1} \chi^{\beta}_{H_2}(e_{H_1}) = |H_1|$. Then according to *proposition* 2 we deduce the result. □

3.3 Dual Characterization with a Regular Action on Inputs

In order to specify the form of the G-perfect nonlinear functions we restrict ourselves to the case of regular actions on the inputs set. Indeed by decreasing the degrees of freedom of the G-perfect nonlinearity we obtain similar results to those in the traditional case.

Theorem 3. *Let (G, X, H) be a triple in which G and H are two f.A.g. and G acts* **regularly** *on a finite nonempty set X. Let $f : X \to H$ and $x_0 \in X$. Then f is G-perfect nonlinear if and only if $f_{x_0} : G \longrightarrow H$ such that $f_{x_0}(\sigma) = f(\sigma.x_0)$ is perfect nonlinear (in the classical way).*

Proof. We will show that for $\sigma \in G \setminus \{e_G\}$ and $\beta \in H$, $|\{x \in X | f(\sigma.x) - f(x) = \beta\}| = |\{\tau \in G | f_{x_0}(\sigma \circ \tau) - f_{x_0}(\tau) = \beta\}|$.
Let $x \in X = \mathcal{O}_G(x_0)$. There exists one and only one $\tau \in G$ such that $x = \tau.x_0$ (since G acts regularly on X). So we have $|\{x \in X | f(\sigma.x) - f(x) = \beta\}| = |\{\tau \in G | f(\sigma \circ \tau.x_0) - f(\tau.x_0) = \beta\}|$ which gives the result. □

The fact that f is G-perfect nonlinear does not depend from the choice of x_0 since the action is regular so each $x \in X$ plays exactly the same role.
The direct consequence below follows : in the regular case, it is possible to carry the notion of G-perfect nonlinearity for functions defined on X to the usual notion of perfect nonlinearity for G-defined maps.

Corollary 1. *Under the same hypothesis, f is G-perfect nonlinear if and only if $\forall x \in X$, $\forall \beta \in H \setminus \{e_H\}$, $\forall \sigma \in G$, $|\widehat{\chi^{\beta}_H \circ f_x}(\sigma)|^2 = |G| = |X|$ (i.e. f_x is generalized bent).*

Note that if we consider the action by translation of a *f.A.g.* G on itself, we find the traditional concept since, according to the previous theorem, a function $f : G \longrightarrow H$ is G-perfect nonlinear if and only if $f_{e_G} : x \in G \mapsto f_{e_G}(x) = f(x + e_G) = f(x) \in H$ is perfect nonlinear in the classical sense.

3.4 Construction of a G-Perfect Nonlinear Function in the regular action case

Let H_1 be a *f.A.g.* and $T(H_1)$ the group of translations of H_1. We denote by $\sigma_\alpha : x \in H_1 \mapsto x + \alpha \in H_1$ the translation associated to $\alpha \in H_1$. Let $\pi \in S(H_1)$

and $G_\pi = \pi T(H_1)\pi^{-1}$ the conjugate group of $T(H_1)$ by π. It is easy to see that G_π acts regularly on H_1 by $\pi \circ \sigma_\alpha \circ \pi^{-1}.x = \pi(\alpha + \pi^{-1}(x))$. Let suppose that it exists $g : H_1 \longrightarrow H_2$ such that g is perfect nonlinear in the classical way. Let define $f : H_1 \longrightarrow H_2$ by $f(x) = g(\pi^{-1}(x))$. We obtain then the following proposition.

Proposition 3. *The function f previously defined is G_π-perfect nonlinear.*

Proof. We denote e_{G_π} by Id. Let $\sigma \in G_\pi \setminus \{Id\}$ and $\beta \in H_2$. We have

$$|\{x \in H_1 | f(\sigma.x) - f(x) = \beta\}| = |\{x \in H_1 | f(\pi \circ \sigma_\alpha \circ \pi^{-1}.x) - f(x) = \beta\}| \quad (8)$$

since it exists one and only one $\alpha \in H_1 \setminus \{e_{H_1}\}$ such that the translation σ_α is conjugated by π with σ. Then it results that

$$\begin{aligned}
(8) &= |\{y \in H_1 | f(\pi(\sigma_\alpha(y))) - f(\pi(y)) = \beta\}| \ (\textit{change of variable} : y = \pi^{-1}(x)) \\
&= |\{y \in H_1 | g(\sigma_\alpha(y)) - g(y) = \beta\}| \\
&= |\{y \in H_1 | g(\alpha + y) - g(y) = \beta\}| \\
&= \frac{|H_1|}{|H_2|} \ (\textit{by perfect nonlinearity of } g).
\end{aligned}$$

That concludes the proof. □

4 Input/Output Group Actions based Perfect Nonlinearity

A natural way to generalize the notion of perfect nonlinearity previously defined consists in taking in account not only group actions on the inputs set of a function but also actions on the outputs set.
Let (G, X, H, Y) be 4-tuple of two *f.A.g.* G, H and two finite nonempty sets X and Y such that G acts **faithfully** on X and H acts **regularly** on Y (by the group homomorphism ψ).

Definition 2. A function $f : X \longrightarrow Y$ is said (G, H)-*perfect nonlinear* if $\forall \sigma \in G \setminus \{e_G\}$, $\forall \tau \in H$, we have

$$|\{x \in X | f(\sigma.x) = \tau.f(x)\}| = \frac{|X|}{|Y|} .$$

The action of H on Y taking the place of the translations of Y, this definition is a direct generalization of the notion of input group actions based perfect nonlinearity of the previous section.
Actually according to the following proposition this notion does not bring anything really new since we can always refer to the Sect. 3 cases.

Proposition 4. *Let $y_0 \in Y$. $f : X \longrightarrow Y$ is (G, H)-perfect nonlinear if and only if $\tilde{f} : X \longrightarrow H$ such that $\tilde{f}(x) = \psi_{y_0}^{-1} \circ f(x)$ (where $\psi_{y_0} : H \longrightarrow Y$ is the orbital function) is G-perfect nonlinear.*

Proof. Let $(\sigma,\tau) \in G \setminus \{e_G\} \times H$. We show that for a fixed $x \in X$, $f(\sigma.x) = \tau.f(x) \Leftrightarrow D_\sigma \tilde{f}(x) = \tilde{f}(\sigma.x) \circ (\tilde{f}(x))^{-1} = \tau$ where $(\tilde{f}(x))^{-1}$ is the inverse of $\tilde{f}(x)$ in H.
We have the following chain of equivalences.
$f(\sigma.x) = \tau.f(x) \Leftrightarrow \tilde{f}(\sigma.x).y_0 = \tau.(\tilde{f}(x).y_0)$ (by definition of $\tilde{f}$) $\Leftrightarrow \tilde{f}(\sigma.x).y_0 = (\tau \circ \tilde{f}(x)).y_0 \Leftrightarrow \tilde{f}(\sigma.x) = (\tau \circ \tilde{f}(x))$ (by *lemma* 2) $\Leftrightarrow \tilde{f}(\sigma.x) \circ (\tilde{f}(x))^{-1} = \tau$.
Then we have $\{x \in X | f(\sigma.x) = \tau.f(x)\} = \{x \in X | \tilde{f}(\sigma.x) \circ (\tilde{f}(x))^{-1} = \tau\}$ which allows us to complete the proof. □

The properties studied in the previous section can then be applied to this kind of functions.

5 Characterization via G-difference sets

In this section we show that G-perfect nonlinear functions from a finite nonempty set X to $\mathbb{F}_2$, with G acting regularly on X, are the characteristic functions of a certain kind of subsets of X similar to difference sets.

Let (G,X) be a couple such that G is *f.A.g.* that acts regularly on X by $\phi : G \longrightarrow S(X)$.
The *support* of a function g from X to $\mathbb{F}_2$ is the set

$$S_g = \{x \in X | g(x) = 1\} .$$

Note that $g = \mathbb{1}_{S_g}$ where $\mathbb{1}_E$ is the characteristic function of a set E.
For any subset A of X we define $\sigma.A \cap A = \{\sigma.x \in X | x \in A\} \cap A$.
The following easy result plays an important role in the sequel.

Theorem 4. *Let $f : X \longrightarrow \mathbb{F}_2$. Then for any $\sigma \in G \setminus \{e_G\}$,*

$$|\{x \in X | D_\sigma f(x) = \beta\}| = \begin{cases} |X| - 2(|S_f| - |\sigma.S_f \cap S_f|) & \text{if } \beta = 0, \\ 2(|S_f| - |\sigma.S_f \cap S_f|) & \text{if } \beta = 1. \end{cases} \quad (9)$$

Proof. It is sufficient to prove that $|S_{D_\sigma f}| = 2(|S_f| - |\sigma.Sf \cap S_f|)$ which is easily checkable. □

A subset D of X is a (v,k,λ) *difference set* if $|X| = v$, $|D| = k$ and the equation $x - y = g$ has exactly λ solutions in $(x,y) \in D^2$ for every nonzero element $g \in G$. These sets are very important for the study of perfect nonlinear $\mathbb{F}_2$-valued functions since these functions are the characteristic functions of a certain kind of difference sets. In order to deal with our notion of G-perfect nonlinear functions, we define a similar combinatorial object

Definition 3. Let $v = |X|$. Let $D \subset X$ and $k = |D|$. D is called a $G - (v,k,\lambda)$ *difference set* of X if $\forall \sigma \in G \setminus \{e_G\}$, the equation

$$x = \sigma.y$$

has exactly λ distinct solutions $(x,y) \in D^2$.

The link between classical and G- difference sets is established by the following proposition.

Proposition 5. *Let D be $G-(v,k,\lambda)$ difference set of X and $x_0 \in X$. Then $\phi_{x_0}^{-1}(D) = \{\sigma \in G | \sigma.x_0 \in D\}$ is a (v,k,λ)-difference set of G.*

Proof. $|\phi_{x_0}^{-1}(D)| = |D| = k$ since the orbital function is bijective and $|G| = |X| = v$.
We denote by ψ_{x_0} the inverse bijection of ϕ_{x_0}.
Let $(x,y) \in D^2$ and $\sigma \in G \setminus \{e_G\}$. We have $x = \sigma.y \Leftrightarrow \psi_{x_0}(x).x_0 = \sigma \circ \psi_{x_0}(y).x_0 \Leftrightarrow \psi_{x_0}(x) = \sigma \circ \psi_{x_0}(y)$ (by *lemma* 2) $\Leftrightarrow \psi_{x_0}(x) \circ (\psi_{x_0}(y))^{-1} = \sigma$.
That allows us to infer the result. □

By applying *theorem* 4 on a characteristic function of a G-difference set we obtain the following theorem.

Theorem 5. *Let D be a $G-(v,k,\lambda)$ difference set of X. Then*

1. *for any $\sigma \in G \setminus e_G$,*

$$|\{x \in X | D_\sigma \mathbb{1}_D(x) = \beta\}| = \begin{cases} v - 2(k-\lambda) & \text{if } \beta = 0, \\ 2(k-\lambda) & \text{if } \beta = 1. \end{cases} \tag{10}$$

2. $\max\limits_{\sigma \in G \setminus \{e_G\}} \max\limits_{\beta \in \mathbb{F}_2} |\{x \in X | D_\sigma \mathbb{1}_D(x) = \beta\}| = \max\{v - 2(k-\lambda), 2(k-\lambda)\}$.

Proof. According to the previous theorem, we obtain

$$|\{x \in X | D_\sigma \mathbb{1}_D(x) = \beta\}| = \begin{cases} |X| - 2(|S_{\mathbb{1}_D}| - |\sigma.S_{\mathbb{1}_D} \cap S_{\mathbb{1}_D}|) & \text{if } \beta = 0, \\ 2(|S_{\mathbb{1}_D}| - |\sigma.S_{\mathbb{1}_D} \cap S_{\mathbb{1}_D}|) & \text{if } \beta = 1. \end{cases} \tag{11}$$

Since $v = |X|$, $|S_{\mathbb{1}_D}| = |D| = k$ and $\lambda = |\sigma.D \cap D|$ we deduce the result. □

By the following theorem we obtain all the G-perfect nonlinear $\mathbb{F}_2$-valued functions.

Theorem 6. *Let $f : X \longrightarrow \mathbb{F}_2$. Then f is G-perfect nonlinear if and only if S_f is a $G-(4u^2, 2u^2 \pm u, u(u \pm 1))$ difference set of X where $|X| = 4u^2$.*

Proof. We begin with the direct implication. f is G-perfect nonlinear implies that $\forall(\sigma,\beta) \in (G \setminus \{e_G\}) \times \mathbb{F}_2$, $|\{x \in X | D_\sigma f(x) = \beta\}| = \frac{|X|}{2} = 2(|S_f| - |\sigma.S_f \cap S_f|)$ (according to *theorem* 4). Then $\forall \sigma \in G \setminus \{e_G\}$, $|\sigma.S_f \cap S_f|$ is constant. Let denote by λ this constant. Since $\forall \sigma \in G \setminus \{e_G\}$, there are $|\sigma.S_f \cap S_f| = \lambda$ solutions $(x,y) \in S_f^2$ to the equation $x = \sigma.y$, S_f is a $G-(|X|, |S_f|, \lambda)$ difference set of X. According to *proposition* 5, for any $x_0 \in X$, $\phi_{x_0}^{-1}(S_f)$ is a $(|X|, |S_f|, \lambda)$ difference set of X. Since $|X| = 4(|S_f| - |\sigma.S_f \cap S_f|)$, we have $|X| \equiv 0 \pmod 4$ and in accordance with [4] such a difference set exist only if $|X| = 4u^2$ (for a certain u) and its parameters have the form $(4u^2, 2u^2 \pm u, u(u \pm 1))$ (it is an Hadamard difference set).
Let us prove the second implication.
Suppose that S_f is a $G-(4u^2, 2u^2 \pm u, u(u \pm 1))$ difference set of X where $|X| = 4u^2$. According to the previous theorem by replacing $\mathbb{1}_D$ by $f = \mathbb{1}_{S_f}$ and (v,k,λ) by the actual parameters of S_f we conclude the proof. □

As in the classical case the Hadamard-like G-difference sets determines all the $\mathbb{F}_2$-valued perfect nonlinear functions. Moreover the theorem above implies the non-existence following result. Let H be a *f.A.g.* and $\gamma \in S(H)$ a cycle of size $|H|$. Let $\langle\gamma\rangle$ be the group generated by γ. Then $|\langle\gamma\rangle| = |H|$ (since the order of γ is $|H|$) and $\langle\gamma\rangle$ acts regularly on H. It is easy to prove the second fact. Let $(x, y) \in H^2$. These two elements appear in the cycle γ then it exists k such that $0 \leq k \leq |H| - 1$ that satisfies $\gamma^k(x) = y$. We now suppose that $H = \mathbb{F}_2^m$, $|H| = 4u^2$ and $u > 1$. Then we wonder if there exist $\langle\gamma\rangle$-perfect nonlinear $\mathbb{F}_2$-valued functions on H. The answer is negative. Indeed (see [9]) an Hadamard difference set exists in such a 2-group of cardinality $4u^2$ if and only if the exponent of the group is less than or equal to $4u$ which is not the case for $\langle\gamma\rangle$ since the exponent of $\langle\gamma\rangle$ is $4u^2 > 4u$.
This last result proves the difference between the usual bent functions and G-perfect nonlinear ones.

6 Conclusion and Further Works

The generalization of the notion of perfect nonlinearity has been introduced in this paper by considering abstract regular or faithful actions on finite Abelian groups - that are the input and output sets of functions - rather than the simple action by translation (or multiplication) of groups on themselves. Whereas the traditional concept describe only one kind of combinatorial objects, our notion is more flexible and graduated by considering faithful actions. As in the classical case we have presented a dual characterization by the Fourier transform with an energy conservation-like formula. In addition some links between our new concepts and the original ones have been given. Finally we have obtained a complete characterization of $\mathbb{F}_2$-valued generalized perfect nonlinear functions (when the input group Action is regular) via new combinatorial objects that we called *G-difference sets*.
Concerning the continuation of our works, in the cases where traditional perfect nonlinear functions do not exist, we should estimate the maximal size of groups G acting faithfully such that G-perfect nonlinear functions exist. It follows that we could then approximate the notion of perfect nonlinearity by the less strong nonlinear property depending of a faithful input group action. Moreover we should also consider the weaker concept of *group actions based bent functions i.e.* those functions $f : H_1 \longrightarrow H_2$ such that for all $x \in H_1$, $f_x : \sigma \in G \longrightarrow f(\sigma.x) \in H_2$ is bent (where G acts regularly or at least faithfully on H_2) since this kind of functions has naturally occurred in our context.

References

[1] E. Biham, A. Shamir : Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1, pp. 3-72, 1991

[2] C. Carlet, C. Ding : Highly nonlinear mappings. In *Journal of Complexity*, Volume 20, Issue 2-3, Special issue on Coding and Cryptography, pp. 205-244, 2004

[3] J. Daemen, V. Rijmen : The Design of Rijndael. AES - The Advanced Encryption Standard, Ed. Springer-Verlag, Berlin, 2002

[4] D. Jungnickel : Difference sets. In J. Dinitz and D. R. Stinson Eds., Contemporary Design Theory : A Collection of Surveys, John Wiley & Sons, 1992

[5] O.A. Logachev, A.A. Salnikov, V.V. Yashchenko : Bent functions on a finite Abelian group, *Discrete Math. Appl.* 7(6), pp. 547-564, 1997

[6] M. Matsui : Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology, Proc. Eurocrypt'93, LNCS 809*, pp. 1-17, 1994

[7] K. Nyberg : Perfect nonlinear S-boxes. In *Lecture Notes in Computer Science, Advances in Cryptology - EUROCRYPT'91*, volume 547, pp. 378-385. Springer-Verlag, 1991

[8] L. Poinsot, S. Harari : Generalized Boolean Bent Functions. In *Lecture Notes in Computer Science, Progress in Cryptology - INDOCRYPT 2004*, to appear in December 2004

[9] R. J. Turyn : Character sums and difference sets. In *Pacific J. Math.* 15, pp. 319-346, 1965

Biography

I am Laurent Poinsot, a PhD student in Mathematics. My advisor is the professor Sami Harari From l'Université du Sud Toulon-Var. We work together on the very relevant cryptographic notions of perfect nonlinearity and bentness in order to find new solidity criteria for Boolean functions.