Generalized Boolean bent functions

Laurent Poinsot, Sami Harari

Generalized Boolean Bent Functions

Laurent Poinsot and Sami Harari

Institut des Sciences de l'Ingénieur de Toulon et du Var (I.S.I.T.V.)
Université du Sud, Toulon-Var (U.S.T.V.)
Laboratoire S.I.S.
Avenue G. Pompidou
BP 56
83162 La Valette du Var cédex, France
{laurent.poinsot,sami.harari}@univ-tln.fr

Abstract. The notions of perfect nonlinearity and bent functions are closely dependent on the action of the group of translations over $\mathbb{F}_2^m$. Extending the idea to more generalized groups of involutions without fixed points gives a larger framework to the previous notions. In this paper we largely develop this concept to define G-perfect nonlinearity and G-bent functions, where G is an Abelian group of involutions, and to show their equivalence as in the classical case.

1 Introduction

The security of secret-key cryptosystems is essentially based on the resistance to two famous attacks, *differential* [1] and *linear cryptanalysis* [2].
On the one hand the functions that exhibit the best resistance to differential cryptanalysis, called *perfect nonlinear*, satisfy to the following conditions

$$\forall \alpha \in \mathbb{F}_2^m \setminus \{0_{\mathbb{F}_2^m}\}, \forall \beta \in \mathbb{F}_2^n, |\{x \in \mathbb{F}_2^m | f(x \oplus \alpha) \oplus f(x) = \beta\}| = 2^{m-n} \quad (1)$$

where $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ and $\oplus$ is the sum over $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$ (the component-wise modulo-two sum). Then for all $\alpha \in \mathbb{F}_2^m \setminus \{0_{\mathbb{F}_2^m}\}$, the derivative of f in the direction α, $d_\alpha f : x \in \mathbb{F}_2^m \mapsto f(x \oplus \alpha) \oplus f(x)$, is uniformly distributed over $\mathbb{F}_2^n$.
On the other hand the linear resistant functions, called *bent functions*, are defined with respect to their (discrete) Fourier transform,

$$\forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}, \forall \alpha \in \mathbb{F}_2^m, \widehat{\chi_{\mathbb{F}_2^n}^\beta \circ f}(\alpha) = \pm 2^{\frac{m}{2}} \quad (2)$$

where $\chi_{\mathbb{F}_2^n}^\beta : y \in \mathbb{F}_2^n \mapsto (-1)^{\beta . y} \in \{\pm 1\}$ is a character, the symbol "." denotes the (canonical) dot-product over $\mathbb{F}_2^n$, $\widehat{F}$ is the Fourier transform of a function $F : \mathbb{F}_2^m \longrightarrow \mathbb{C}$ and $\circ$ is the composition of functions.
Actually these two notions are equivalent as pointed out by Nyberg in [3] since

a function is perfect nonlinear if and only if it is bent.

The two corresponding attacks are dual one from the other by the Fourier transform.

Now let σ_α be the translation by α over $\mathbb{F}_2^m$. We can naturally rewrite the formula (1)

$$\forall \alpha \in \mathbb{F}_2^m \setminus \{0_{\mathbb{F}_2^m}\}, \forall \beta \in \mathbb{F}_2^n, |\{x \in \mathbb{F}_2^m | f(\sigma_\alpha(x)) \oplus f(x) = \beta\}| = 2^{m-n} \quad . \qquad (3)$$

Thus the concept of perfect nonlinearity is closely linked with the action of the translations over $\mathbb{F}_2^m$.

There is a natural way to extend at the same time the notions of perfect nonlinearity and, by duality, that of bent functions. Suppose G is an Abelian group of involutions without fixed points of $\mathbb{F}_2^m$, then we can introduce the notion of *G-perfect nonlinearity* of f by considering the action of G over $\mathbb{F}_2^m$ as follows

$$\forall \sigma \in G \setminus \{Id\}, \forall \beta \in \mathbb{F}_2^n, |\{x \in \mathbb{F}_2^m | f(\sigma(x)) \oplus f(x) = \beta\}| = 2^{m-n} \qquad (4)$$

where Id is the identity function of $\mathbb{F}_2^m$.

1.1 Our Contributions

In this paper we extend the notion of perfect nonlinearity by using involutions instead of simple translations. We also establish a dual version of G-perfect nonlinearity, as in the classical case, in terms of Fourier transform, that allows us to generalize the notion of bent functions. We exhibit some relations between the original and new concepts. In order to summarize we offer a larger framework to the concepts of perfect nonlinearity and bent functions.

1.2 Organization of the Paper

The continuation of this paper is organized as follows. In the next section, we give the basic definitions from dual groups to Abelian groups of involutions that are used along the paper. In Sect. 3, we introduce our new notion of G-perfect nonlinearity based on involutions. Then we study its duality through the Fourier transform in order to extend the concept of boolean bent functions. In addition, a construction of a generalized bent function is proposed. The Sect. 4 is devoted to the links between classical and new notions. Finally in Sect. 5, we show as in the classical case that our perfect nonlinear functions reach the maximum distance to a certain kind of affine functions.

2 Notations and Preliminaries

In this part we recall some essential concepts and results on dual groups, Fourier transform and bent functions. We also introduce several properties of involutions without fixed points.

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

The definitions and results of this paragraph come from [4] and [5].
Let G be a finite Abelian group. 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 Abelian group, 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 $G = \mathbb{F}_2^m$, $\chi_{\mathbb{F}_2^m}^\alpha : x \in \mathbb{F}_2^m \mapsto (-1)^{\alpha.x}$. Until the end of this paper, any time we refer to a finite Abelian group, we suppose that an isomorphism from it to its dual group 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 finite Abelian groups. 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

$$d_\alpha f : x \in G_1 \mapsto f(\alpha + x) - f(x) \in G_2 \tag{5}$$

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

$$\forall \alpha \in G_1 \setminus \{e_{G_1}\}, \forall \beta \in G_2, |\{x \in G_1 | d_\alpha f(x) = \beta\}| = \frac{|G_1|}{|G_2|} \ . \tag{6}$$

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*

$$\widehat{\chi_{G_2}^\beta \circ f}(e_{G_1}) = 0 \ . \tag{7}$$

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

Theorem 1. *$f : G_1 \longrightarrow G_2$ is perfect nonlinear if and only if it is 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 Involutions without Fixed Points

Let $S(\mathbb{F}_2^m)$ be the symmetric group of $\mathbb{F}_2^m$. Let $\sigma \in S(\mathbb{F}_2^m)$. σ is an *involution* if $\sigma^2 = \sigma \circ \sigma = Id$ or in other terms $\sigma^{-1} = \sigma$. Moreover σ is *without fixed points* if $\forall x \in \mathbb{F}_2^m$, $\sigma x \neq x$. We denote by $Inv(\mathbb{F}_2^m)$ the set of *involutions without fixed points*. By definition, we can easily see that an element of $Inv(\mathbb{F}_2^m)$ is the product of 2^{m-1} transpositions with disjoint supports. So $Inv(\mathbb{F}_2^m)$ is a conjugacy class of $S(\mathbb{F}_2^m)$. Its cardinality is given by the formula $\frac{2^m!}{2^{m-1}!2^{2^m-1}}$.

Let $T(\mathbb{F}_2^m)$ be the (Abelian) group of translations of $\mathbb{F}_2^m$ (subgroup of $S(\mathbb{F}_2^m)$). Then we can easily check that $T(\mathbb{F}_2^m) \setminus \{Id\} \subset Inv(\mathbb{F}_2^m)$ and since for $m > 2$, $|Inv(\mathbb{F}_2^m)| > |T(\mathbb{F}_2^m)| = 2^m$ there exists (lots of) nonlinear involutions without fixed points.

In the sequel we adopt the following usual notations, for $(\sigma, \tau) \in S(\mathbb{F}_2^m)^2$, $\sigma\tau$ and σx denote respectively $\sigma \circ \tau$ and $\sigma(x)$. The small Greek letters are kept to name the permutations and we use the small Roman letters to denote the points of $\mathbb{F}_2^m$.

We have these interesting and useful properties concerning involutions without fixed points.

Property 1. Let G be a subgroup of $S(\mathbb{F}_2^m)$ such that $G \setminus \{Id\} \subset Inv(\mathbb{F}_2^m)$ (such a group is called a *group of involutions of* $\mathbb{F}_2^m$). Then G is Abelian.

Proof. Let $(\sigma, \tau) \in G^2$. Since $\sigma\tau \in G$ then either $\sigma\tau = Id$ or $\sigma\tau \in Inv(\mathbb{F}_2^m)$. In the first case, $\sigma = \tau^{-1} = \tau$ then $\sigma\tau = \tau\sigma$. In the second case, $(\sigma\tau)^2 = Id \Leftrightarrow \sigma\tau\sigma\tau = Id \Leftrightarrow \tau\sigma\tau = \sigma^{-1} = \sigma \Leftrightarrow \sigma\tau = \tau^{-1}\sigma = \tau\sigma$.
The property follows. □

Property 2. Let G be a group of involutions of $\mathbb{F}_2^m$. Then $|G| \leq 2^m$.

Proof. Suppose on the contrary that $|G| > 2^m$. Then there exists $(\sigma, \tau) \in G^2$ such that $\sigma \neq \tau$ and $\sigma 0_{\mathbb{F}_2^m} = \tau 0_{\mathbb{F}_2^m}$. If not then $f_{0_{\mathbb{F}_2^m}} : \sigma \in G \mapsto f_{0_{\mathbb{F}_2^m}}(\sigma) = \sigma 0_{\mathbb{F}_2^m} \in \mathbb{F}_2^m$ is injective and $|\{f_{0_{\mathbb{F}_2^m}}(\sigma) | \sigma \in G\}| = |G| \leq |\mathbb{F}_2^m| = 2^m$ which is impossible by hypothesis. So let $(\sigma, \tau) \in G^2$ such that $\sigma \neq \tau$ and $\sigma 0_{\mathbb{F}_2^m} = \tau 0_{\mathbb{F}_2^m}$. Then $\sigma\tau 0_{\mathbb{F}_2^m} = \sigma\sigma 0_{\mathbb{F}_2^m} = \sigma^2 0_{\mathbb{F}_2^m} = 0_{\mathbb{F}_2^m}$. Consequently $0_{\mathbb{F}_2^m}$ is a fixed point for $\sigma\tau$. Since $\sigma \neq \tau$ then $\sigma\tau \neq Id$ and $\sigma\tau$ has no fixed point. Thus we have a contradiction with the assumption that $|G| > 2^m$. □

Property 3. For $m > 2$, there exists G a group of involutions of $\mathbb{F}_2^m$ such that $|G| = 2^m$ and $G \neq T(\mathbb{F}_2^m)$.

Proof. Let $\alpha \in \mathbb{F}_2^m \setminus \{0_{\mathbb{F}_2^m}\}$ and $\sigma_\alpha \in T(\mathbb{F}_2^m)$ the corresponding translation. Let $\tau \in Inv(\mathbb{F}_2^m) \setminus T(\mathbb{F}_2^m)$ (such a nonlinear involution exists since $m > 2$). Since τ and σ_α are conjugate, it exists $\pi \in S(\mathbb{F}_2^m)$ such that $\tau = \pi\sigma_\alpha\pi^{-1}$. It is easy to see that $\pi T(\mathbb{F}_2^m)\pi^{-1}$ is a group of involutions (a *conjugate group of* $T(\mathbb{F}_2^m)$) such that $|\pi T(\mathbb{F}_2^m)\pi^{-1}| = 2^m$ and $\pi T(\mathbb{F}_2^m)\pi^{-1} \neq T(\mathbb{F}_2^m)$ (since $\tau \in \pi T(\mathbb{F}_2^m)\pi^{-1}$ and $\tau \notin T(\mathbb{F}_2^m)$). □

Remark 1. In the previous property, the fact "$m > 2$" is needed to obtain a group of involutions G such that $|G| = 2^m$ **and** $G \neq T(\mathbb{F}_2^m)$. If $m = 1$ or $m = 2$ we have only one group of involutions of maximal size $G = T(\mathbb{F}_2)$ or $G = T(\mathbb{F}_2^2)$.

We call *maximal group of involutions* of $\mathbb{F}_2^m$ a group of involutions G of $\mathbb{F}_2^m$ such that $|G| = 2^m$.

Property 4. Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Then the action $\phi : G \longrightarrow S(\mathbb{F}_2^m)$ such that $\phi(\sigma) : x \mapsto \sigma x$ is simply transitive.

Proof. Let us define for $x \in \mathbb{F}_2^m$ the orbital function $f_x : \sigma \in G \mapsto f_x(\sigma) = \phi(\sigma)(x) = \sigma x \in \mathbb{F}_2^m$. Then for all $x \in \mathbb{F}_2^m$, f_x is injective. Indeed let $(\sigma, \tau) \in G^2$ such that $\sigma \neq \tau$. If $f_x(\sigma) = f_x(\tau)$ then we have the following chain of equivalences $\sigma x = \tau x \Leftrightarrow \tau\sigma x = x \Leftrightarrow x$ is a fixed point of $\tau\sigma$ which is impossible since $\tau\sigma \neq Id$. In addition we have $|G| = |\mathbb{F}_2^m|$ then f_x is bijective. That concludes the proof.□

Finally for a group of involutions G of $\mathbb{F}_2^m$, since the exponent of G is 2 (all the elements distinct from the identity have an order two) and it is an Abelian group, the dual group $\widehat{G}$ is the set of homomorphisms from G to $\{\pm 1\}$ and is isomorphic to G.

3 Generalized Boolean Bent Functions

In this section we introduce a new notion of perfect nonlinearity that extends and offers a larger framework for the classical one. We also study its dual version through the Fourier transform which leads us to introduce a generalized definition for the concept of bent functions.

3.1 Definitions and Properties

Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$. We define the *derivative of f in direction $\sigma \in G$* by

$$\begin{aligned} D_\sigma f : \mathbb{F}_2^m &\longrightarrow \mathbb{F}_2^n \\ x &\mapsto D_\sigma f(x) = f(\sigma x) \oplus f(x) \ . \end{aligned} \tag{8}$$

We define $\Delta_f = \sup_{\sigma \neq Id, \beta} |\{x \in \mathbb{F}_2^m | D_\sigma f(x) = \beta\}|$.
We have the following bound for Δ_f.

Theorem 2. *For any function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$, $\Delta_f \geq 2^{m-n}$.*

Proof. For each fixed $\sigma \in G \setminus \{Id\}$, the collection of sets $\{\{x \in \mathbb{F}_2^m | D_\sigma f(x) = \beta\}\}_{\beta \in \mathbb{F}_2^n}$ is a partition of $\mathbb{F}_2^m$. Then $\sum_{\beta \in \mathbb{F}_2^n} |\{x \in \mathbb{F}_2^m | D_\sigma f(x) = \beta\}| = 2^m$, which implies the result. □

Definition 1. *A function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ is G-perfect nonlinear if $\Delta_f = 2^{m-n}$.*

According to the previous theorem, for a G-perfect nonlinear function f, we have

$$\Delta_f = \inf_{g:\mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n} \Delta_g \ . \tag{9}$$

We can state a first result similar to the traditional case.

Theorem 3. *$f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ is G-perfect nonlinear if and only if for all $\sigma \in G \setminus \{Id\}$, the derivative $D_\sigma f$ is balanced.*

Proof. f is G-perfect nonlinear if and only if the maximum of the sequence of integers $\{|\{x \in \mathbb{F}_2^m | D_\sigma f(x) = \beta\}|\}_{\sigma \in G \setminus \{Id\}, \beta \in \mathbb{F}_2^n}$ is equal to its mean. This is possible if and only if the sequence is constant. Then the constant must be 2^{m-n} which ensures the result. □

From the theorem above we obtain the following immediate results which embeds classical notions in our framework.

Proposition 2. *Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$. f is $T(\mathbb{F}_2^m)$-perfect nonlinear if and only if f is perfect nonlinear in the classical way.*

Proof. f is $T(\mathbb{F}_2^m)$-perfect nonlinear if and only if $D_{\sigma_\alpha} f$ is balanced for every $\sigma_\alpha \in T(\mathbb{F}_2^m) \setminus \{Id\}$ if and only if $D_{\sigma_\alpha} f$ is balanced for every $\alpha \in \mathbb{F}_2^m \setminus \{0_{\mathbb{F}_2^m}\}$. We conclude the proof since $D_{\sigma_\alpha} f(x) = d_\alpha f(x)$ for all $x \in \mathbb{F}_2^m$. □

We now develop the dual description of G-perfect nonlinear functions through the study of their Fourier transform.
Let f and g be two functions from $\mathbb{F}_2^m$ to $\mathbb{R}$. We define

$$\begin{aligned} \Phi_{f,g} : G &\longrightarrow \mathbb{R} \\ \sigma &\mapsto \Phi_{f,g}(\sigma) = \sum_{x \in \mathbb{F}_2^m} f(x) g(\sigma x) \end{aligned} \tag{10}$$

which can be seen as a kind of convolution product with respect to the action of G over $\mathbb{F}_2^m$. Let us compute its Fourier transform. Let $\sigma \in G$.

$$\begin{aligned} \widehat{\Phi_{f,g}}(\sigma) &= \sum_{\tau \in G} \Phi_{f,g}(\tau) \chi_G^\sigma(\tau) \\ &= \sum_{\tau \in G} \sum_{x \in \mathbb{F}_2^m} f(x) g(\tau x) \chi_G^\sigma(\tau) \\ &= \sum_{x \in \mathbb{F}_2^m} f(x) \sum_{\tau \in G} g(\tau x) \chi_G^\sigma(\tau) \ . \end{aligned} \tag{11}$$

Moreover the sum "$\sum_{\tau \in G} g(\tau x) \chi_G^\sigma(\tau)$" is invariant by translations [1] over G *i.e.* $\forall \pi \in G$, $\sum_{\tau \in G} g(\tau x) \chi_G^\sigma(\tau) = \sum_{\tau \in G} g(\tau \pi x) \chi_G^\sigma(\tau \pi) = \sum_{\tau \in G} g(\tau \pi x) \chi_G^\sigma(\tau) \chi_G^\sigma(\pi)$. Then

[1] $\tau \in G \mapsto \tau\pi \in G$ is the translation by $\pi \in G$.

we have

$$
\begin{aligned}
(11) &= \sum_{x\in\mathbb{F}_2^m} f(x)\chi_G^\sigma(\pi)\sum_{\tau\in G} g(\tau\pi x)\chi_G^\sigma(\tau) \\
&= \sum_{x\in\mathbb{F}_2^m} f(\pi x)\chi_G^\sigma(\pi)\sum_{\tau\in G} g(\tau x)\chi_G^\sigma(\tau) \ (\textit{since } \pi^{-1}=\pi) \\
&= \sum_{x\in\mathbb{F}_2^m} f(\pi x)\chi_G^\sigma(\pi)\widehat{g_x}(\sigma) \qquad (12)
\end{aligned}
$$

where $g_x : G \longrightarrow \mathbb{R}$ such that $g_x(\sigma) = g(\sigma x)$. Since (12) is true for all $\pi \in G$, by integration over G, we obtain

$$
\begin{aligned}
\sum_{\pi\in G}\widehat{\Phi_{f,g}}(\sigma) = |G|\widehat{\Phi_{f,g}}(\sigma) &= 2^m\widehat{\Phi_{f,g}}(\sigma) \\
&= \sum_{x\in\mathbb{F}_2^m}\sum_{\pi\in G} f(\pi x)\chi_G^\sigma(\pi)\widehat{g_x}(\sigma) \\
&= \sum_{x\in\mathbb{F}_2^m}\widehat{f_x}(\sigma)\widehat{g_x}(\sigma) \ . \qquad (13)
\end{aligned}
$$

And finally this gives us

$$
\forall\sigma\in G,\ \widehat{\Phi_{f,g}}(\sigma) = \frac{1}{2^m}\sum_{x\in\mathbb{F}_2^m}\widehat{f_x}(\sigma)\widehat{g_x}(\sigma) \qquad (14)
$$

which is equivalent, in our context, to the trivialization of the convolution product by the Fourier transform.

Proposition 3. *Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$, $\beta \in \mathbb{F}_2^n$ and $F_{\beta,f} : G \longrightarrow \mathbb{R}$ such that $F_{\beta,f}(\sigma) = \widehat{\chi^\beta_{\mathbb{F}_2^n}\circ D_\sigma f}(0_{\mathbb{F}_2^m})$. Then we have*

$$
\forall\sigma\in G,\ \widehat{F_{\beta,f}}(\sigma) = \frac{1}{2^m}\sum_{x\in\mathbb{F}_2^m}(\widehat{\chi^\beta_{\mathbb{F}_2^n}\circ f_x}(\sigma))^2.
$$

Proof. First of all, $F_{\beta,f}$ is real-valued since the characters of $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$ are $\{\pm1\}$-valued.
Let us compute the Fourier transform of $F_{\beta,f}$.

$$
\begin{aligned}
\widehat{F_{\beta,f}}(\sigma) &= \sum_{\tau\in G} F_{\beta,f}(\tau)\chi_G^\sigma(\tau) \\
&= \sum_{\tau\in G}\sum_{x\in\mathbb{F}_2^m}(\chi^\beta_{\mathbb{F}_2^n}\circ D_\tau f)(x)\chi_G^\sigma(\tau) \\
&= \sum_{\tau\in G}\sum_{x\in\mathbb{F}_2^m}\chi^\beta_{\mathbb{F}_2^n}(f(x)\oplus f(\tau x))\chi_G^\sigma(\tau) \\
&= \sum_{\tau\in G}\sum_{x\in\mathbb{F}_2^m}(\chi^\beta_{\mathbb{F}_2^n}\circ f)(x)(\chi^\beta_{\mathbb{F}_2^n}\circ f)(\tau x)\chi_G^\sigma(\tau)
\end{aligned}
$$

$$= \sum_{\tau \in G} \Phi_{\chi^{\beta}_{\mathbb{F}_2^n} \circ f, \chi^{\beta}_{\mathbb{F}_2^n} \circ f}(\tau) \chi^{\sigma}_{G}(\tau)$$
$$= \widehat{\Phi_{\chi^{\beta}_{\mathbb{F}_2^n} \circ f, \chi^{\beta}_{\mathbb{F}_2^n} \circ f}}(\sigma)$$
$$= \frac{1}{2^m} \sum_{x \in \mathbb{F}_2^m} (\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f})_x(\sigma)(\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f})_x(\sigma) \ (\textit{according to } (14))$$
$$= \frac{1}{2^m} \sum_{x \in \mathbb{F}_2^m} ((\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f})_x(\sigma))^2$$
$$= \frac{1}{2^m} \sum_{x \in \mathbb{F}_2^m} (\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma))^2 \ .$$

□

Then we have one of the most important theorem which allows us to define an extended notion of bent functions.

Theorem 4. *Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$. f is G-perfect nonlinear if and only if $\forall \sigma \in G$, $\forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}$,*

$$\sum_{x \in \mathbb{F}_2^m} (\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma))^2 = 2^{2m} \ .$$

Proof. f is G-perfect non linear $\Leftrightarrow \forall \sigma \in G \setminus \{Id\}$, $D_\sigma f$ is balanced over $\mathbb{F}_2^m$
$\Leftrightarrow \forall \sigma \in G \setminus \{Id\}$, $\forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}$, $\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ D_\sigma f}(0_{\mathbb{F}_2^m}) = 0$ (by *proposition* 1)
$\Leftrightarrow \forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}$, $\forall \sigma \in G \setminus \{Id\}$, $F_{\beta,f}(\sigma) = 0$
$\Leftrightarrow \forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}$, $\widehat{F_{\beta,f}}$ is constant over G (according to *lemma* 1).
By Parseval equation we have $\frac{1}{2^m} \sum_{\sigma \in G} (\widehat{F_{\beta,f}}(\sigma))^2 = \sum_{\sigma \in G} (F_{\beta,f}(\sigma))^2 = (F_{\beta,f}(Id))^2$.
Thus since $\widehat{F_{\beta,f}}$ is constant, $(\widehat{F_{\beta,f}}(\sigma))^2 = (F_{\beta,f}(Id))^2$ for all $\sigma \in G$. Moreover $F_{\beta,f}(Id) = \widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ D_{Id} f}(0_{\mathbb{F}_2^m}) = \sum_{x \in \mathbb{F}_2^m} \chi^{\beta}_{\mathbb{F}_2^m}(0_{\mathbb{F}_2^m}) = 2^m$. Then according to *proposition* 3 we deduce the result. □

We can then define the new boolean bent functions by the duality through the Fourier transform previously exhibited as follows.

Definition 2. *Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$. f is called G-bent if $\forall \sigma \in G$, $\forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}$, $\sum_{x \in \mathbb{F}_2^m} (\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma))^2 = 2^{2m}$.*

By this way we keep the equivalence (by *theorem* 4) between the new notions of perfect nonlinearity and bent functions as it is the case for the original concepts.

3.2 Construction of a G-Perfect Nonlinear Function

Let $\pi \in S(\mathbb{F}_2^m)$ and $G_\pi = \pi T(\mathbb{F}_2^m)\pi^{-1}$ the conjugate group of $T(\mathbb{F}_2^m)$ by π (it is a maximal group of involutions). Suppose that there exists $g : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ such that g is perfect nonlinear in the classical way (so g is also bent in the classical way). Let define $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ by $f(x) = g(\pi^{-1}x)$. We have then the following proposition.

Proposition 4. *The function f previously defined is G_π-perfect nonlinear.*

Proof. Let $\sigma \in G_\pi \setminus \{Id\}$ and $\beta \in \mathbb{F}_2^n$. We have

$$|\{x \in \mathbb{F}_2^m | f(\sigma x) \oplus f(x) = \beta\}| = |\{x \in \mathbb{F}_2^m | f(\pi\sigma_\alpha\pi^{-1}x) \oplus f(x) = \beta\}| \qquad (15)$$

since it exists one and only one $\alpha \in \mathbb{F}_2^m \setminus \{0_{\mathbb{F}_2^m}\}$ such that the translation σ_α is conjugated by π with σ. Then we have

$$\begin{aligned}(15) &= |\{y \in \mathbb{F}_2^m | f(\pi\sigma_\alpha y) \oplus f(\pi y) = \beta\}| \text{ (change of variable : } y = \pi^{-1}x) \\ &= |\{y \in \mathbb{F}_2^m | g(\sigma_\alpha y) \oplus g(y) = \beta\}| \\ &= 2^{m-n} \text{ (by perfect nonlinearity of g) .}\end{aligned}$$

That concludes the proof. □

4 Links between Classical and New Notions

In this section we present some relations between our new notions and the classical ones.

Theorem 5. *Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$. f is G-perfect nonlinear if and only if $\forall x \in \mathbb{F}_2^m$, $f_x : G \longrightarrow \mathbb{F}_2^n$ such that $f_x(\sigma) = f(\sigma x)$ is perfect nonlinear in the traditional sense.*

Proof.

⇒) Suppose that f is G-perfect nonlinear. We have to prove that $\forall x \in \mathbb{F}_2^m$, $\forall \sigma \in G \setminus \{Id\}$ and $\forall \beta \in \mathbb{F}_2^n$,

$$|\{\tau \in G | f_x(\sigma\tau) \oplus f_x(\tau) = \beta\}| = \frac{|G|}{2^n} = 2^{m-n}.$$

We have $|\{\tau \in G | f(\sigma\tau x) \oplus f(\tau x) = \beta\}| = |\{y \in \mathbb{F}_2^m | f(\sigma y) \oplus f(y) = \beta\}|$ by the change of variables $\tau x = y$ (one must remember that $\tau \mapsto \tau x$ is bijective since the action of G on $\mathbb{F}_2^m$ is simply transitive). That concludes the first implication.

⇐) Suppose that $\forall x \in \mathbb{F}_2^m$, f_x is perfect nonlinear in the classical way. Then f_x is bent (also in the original sense) *i.e.* $\forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}$, $|\widehat{\chi_{\mathbb{F}_2^n}^\beta \circ f_x}(\sigma)| = \sqrt{|G|} = 2^{\frac{m}{2}}$. Then we have $\sum_{x \in \mathbb{F}_2^m} (\widehat{\chi_{\mathbb{F}_2^n}^\beta \circ f_x}(\sigma))^2 = \sum_{x \in \mathbb{F}_2^m} |G| = 2^{2m}$. So f is G-perfect nonlinear by *theorem* 4. □

Then we have the immediate following corollary, similar to the traditional case.

Corollary 1. *Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$.*
f is G-perfect nonlinear if and only if $\forall x \in \mathbb{F}_2^m$, $\forall \beta \in \mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}$, $\forall \sigma \in G$, $|\widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\sigma)| = 2^{\frac{m}{2}}$.

5 Distance to "Affine" functions

A well-known result is that bent functions have the maximum distance to the set of affine functions defined by the canonical dot-product. In this section we show a similar result. The bent functions with respect to the extended notion reach the maximum distance between a certain kind of affine functions as in the classical context.

Let f and b be functions from E_1 to E_2 (two sets and E_1 is finite), we define the Hamming distance between f and g by

$$d(f,g) = |\{x \in E_1 | f(x) \neq g(x)\}| \ . \tag{16}$$

If A is a (finite) set of functions from E_1 to E_2 we define the distance of a function $f : E_1 \longrightarrow E_2$ to the set A by

$$d(f,A) = \min_{g \in A} d(f,g) \ . \tag{17}$$

Let G be a maximal group of involutions of $\mathbb{F}_2^m$. We define the set of "*affine functions*" over G as

$$\begin{aligned} \mathcal{A}_G &= \{f : G \longrightarrow \{\pm 1\} | \exists (\lambda, c) \in \widehat{G} \times \{\pm 1\} \ \textit{such that} \ f(\sigma) = c\lambda(\sigma)\} \\ &= \{\pm \chi_G^{\sigma} | \sigma \in G\} \end{aligned}$$

i.e. $\mathcal{A}_G$ is the set of affine forms over G.
Let $(\beta, x) \in (\mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}) \times \mathbb{F}_2^m$. We have

$$\begin{aligned} \widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\sigma) &= \sum_{\tau \in G} \chi_{\mathbb{F}_2^n}^{\beta}(f(\tau x)) \chi_G^{\sigma}(\tau) \\ &= |\{\tau \in G | \chi_{\mathbb{F}_2^n}^{\beta}(f(\tau x)) = \chi_G^{\sigma}(\tau)\}| - |\{\tau \in G | \chi_{\mathbb{F}_2^n}^{\beta}(f(\tau x)) \neq \chi_G^{\sigma}(\tau)\}| \\ &\quad (\textit{since both } \chi_{\mathbb{F}_2^n}^{\beta} \textit{ and } \chi_G^{\sigma} \textit{ are } \{\pm 1\} - \textit{valued}) \\ &= |G| - 2d(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \chi_G^{\sigma}) \ . \end{aligned}$$

Thus we obtain

$$d(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \chi_G^{\sigma}) = 2^{m-1} - \frac{1}{2} \widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\sigma) \ . \tag{18}$$

Let us compute $d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, -\chi^{\sigma}_G)$:

$$\begin{aligned} d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, -\chi^{\sigma}_G) &= |\{\tau \in G | \chi^{\beta}_{\mathbb{F}_2^n}(f(\tau x)) \neq -\chi^{\sigma}_G(\tau)\}| \\ &= |\{\tau \in G | \chi^{\beta}_{\mathbb{F}_2^n}(f(\tau x)) = \chi^{\sigma}_G(\tau)\}| \\ &= |G| - |\{\tau \in G | \chi^{\beta}_{\mathbb{F}_2^n}(f(\tau x)) \neq \chi^{\sigma}_G(\tau)\}| \\ &= |G| - d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \chi^{\sigma}_G) \\ &= 2^{m-1} + \frac{1}{2}\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma) \ . \end{aligned}$$

It follows that $d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \{\pm\chi^{\sigma}_G\}) = \min(\{d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \chi^{\sigma}_G), d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, -\chi^{\sigma}_G)\}) = 2^{m-1} - \frac{1}{2}|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)|$.
Since $\mathcal{A}_G = \cup_{\sigma \in G}\{\pm\chi^{\sigma}_G\}$, we have

$$\begin{aligned} d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \mathcal{A}_G) &= \min_{\alpha \in \mathcal{A}_G} d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \alpha) \\ &= \min_{\sigma \in G} d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \{\pm\chi^{\sigma}_G\}) \\ &= \min_{\sigma \in G}(2^{m-1} - \frac{1}{2}|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)|) \\ &= 2^{m-1} - \frac{1}{2}\max_{\sigma \in G}|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)| \ . \end{aligned} \tag{19}$$

Proposition 5. *Let G be a maximal group of involutions of $\mathbb{F}_2^m$ and $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$.*
f is G-perfect nonlinear if and only if $\forall(\beta, x) \in (\mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}) \times \mathbb{F}_2^m$,

$$d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \mathcal{A}_G) = 2^{m-1} - 2^{\frac{m}{2}-1} \ .$$

Proof.

$\Leftarrow$) Let $g : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$. By Parseval equation, we have $\sum_{\sigma \in G}|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\sigma)|^2 = |G|\sum_{\sigma \in G}|\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x(\sigma)|^2 = |G|^2$ (since $\chi^{\beta}_{\mathbb{F}_2^n}$ is $\{\pm 1\}$-valued). So $\max_{\sigma \in G}|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\sigma)| \geq \sqrt{|G|} = 2^{\frac{m}{2}}$ and then $\inf_{g:\mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n}\max_{\sigma \in G}|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\sigma)| \geq 2^{\frac{m}{2}}$. Moreover suppose that we have $d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \mathcal{A}_G) = 2^{m-1} - 2^{\frac{m}{2}-1}$, then according to formula (19), we deduce that $\forall(\beta, x) \in (\mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}) \times \mathbb{F}_2^m$, $\max_{\sigma \in G}|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)| = 2^{\frac{m}{2}}$. Then $\forall\sigma \in G$, $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)| \leq 2^{\frac{m}{2}}$. The lower absolute bound previously exhibited implies then that $\forall\sigma \in G$, $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)| = 2^{\frac{m}{2}}$. The result is given by *corollary* 1.

$\Rightarrow$) By *corollary* 1, if f is G-perfect nonlinear then $\forall(\beta, x) \in (\mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}) \times \mathbb{F}_2^m$, $\forall \sigma \in G$, $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)| = 2^{\frac{m}{2}}$. Therefore we deduce the result by applying the formula (19). $\square$

Corollary 2. *Let G be a maximal group of involutions of $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$. If f is G-perfect nonlinear then $\forall(\beta, x) \in (\mathbb{F}_2^n \setminus \{0_{\mathbb{F}_2^n}\}) \times \mathbb{F}_2^m$, $\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x$ has the maximal distance to $\mathcal{A}_G$.*

Proof. Suppose f G-perfect nonlinear. The same way as in the proof of *proposition* 5, we deduce the $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\sigma)| = \inf_{g:\mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n} \max_{\sigma \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\sigma)| = 2^{\frac{m}{2}}$. Then $\forall g : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$, according to formula (19),

$$d(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, \mathcal{A}_G) \geq 2^{m-1} - \frac{1}{2} \max_{\sigma \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\sigma)| = d(\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x, \mathcal{A}_G) \ .$$

$\square$

6 Conclusion and Further Works

We have extended both notions of perfect nonlinearity and bent functions, while respecting the equivalence between them, by considering groups of involutions rather than the simple translations. Moreover we have shown that our concepts and the original ones are closely dependent. Finally we have obtained a similar result to the traditional case with regard to the distance to the set of affine functions.
The existence of G-perfect nonlinear functions is proved by our construction of such function in the case where G is a conjugate group of the group of translations $T(\mathbb{F}_2^m)$. A problem remaining to solve is to show if the conjugacy class of $T(\mathbb{F}_2^m)$ is equal to the set of all maximal groups of involutions of $\mathbb{F}_2^m$. If it is not the case, we should also construct a G-bent function for G a group of involutions which is not in the same conjugacy class than $T(\mathbb{F}_2^m)$, or we should prove their nonexistence.

References

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

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

[3] 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

[4] 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

[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