Advances and Applications in Discrete Mathematics
Volume 3, Number 1, 2009, Pages 1-46
Published Online: March 30, 2009
This paper is available online at http://www.pphmj.com
© 2009 Pushpa Publishing House

$\mathrm{GF}(2^n)$-BENT FUNCTIONS

LAURENT POINSOT

Institut Galilée
Université Paris-Nord 13
LIPN-UMR CNRS 7030
France
e-mail: laurent.poinsot@lipn.univ-paris13.fr

Abstract

A function from a finite Abelian group G and with values in the unit circle T of the complex field is called bent if its Fourier transform (i.e., the decomposition of f in the basis of characters of G) has a constant magnitude equals to the number of elements of G. In this contribution we define a modulo 2 notion of characters by allowing the characters of an elementary finite Abelian p-group G to take their values in the multiplicative group $\mathrm{GF}(2^n)^*$ (with $p = 2^n - 1$) of the roots of the unity in the finite field $\mathrm{GF}(2^n)$ with 2^n elements rather than in the complex roots of the unity T. We show that this kind of characters forms an orthogonal basis of the $\mathrm{GF}(2^n)$-vector space of functions from G to $\mathrm{GF}(2^n)$ that permits us to define a modulo 2 version of the Fourier transform (as a decomposition of a vector in this basis of characters). We show that many classical properties of the Fourier transform still hold for this characteristic 2 version. In particular, we can define an appropriate notion of bent functions, called $\mathrm{GF}(2^n)$-bent functions, with respect to this Fourier transform. Finally we construct a class of $\mathrm{GF}(2^n)$-bent functions and we also study their relations with classical and group action versions of perfect nonlinearity.

2000 Mathematics Subject Classification: 20K01.

Keywords and phrases: bent functions, perfect nonlinearity, finite Abelian groups, theory of characters, Fourier transform and group actions.

Received September 29, 2008

1. Introduction

In an r-round iterative block cipher, a ciphertext x_r is obtained from a plaintext x_0 by r iterations of a round function R,

$$x_i = R(x_{i-1}, k_i), \quad 1 \leq i \leq r, \tag{1}$$

where k_i is the ith (secret) round key. Usually such cryptosystems are composed of a linear part and a nonlinear part. The role of the first one is to provide a good level of *diffusion* to the cryptosystem. This requirement has been introduced by Shannon in his 1949 famous paper [14] and means that a small deviation in a plaintext should cause a large change at the ciphertext. The nonlinear part is designed to *confuse* the algebraic relations between plaintexts, ciphertexts and keys. More precisely the nonlinear components, namely the *S-boxes*[1], must provide the resistance against several cryptanalysis such as the famous differential and linear attacks. Introduced by Biham and Shamir [1] the differential attack tries to take advantage of a possible bias in output of an S-box for inputs of a fixed difference. The linear cryptanalysis of Matsui [6] consists in approaching an S-box by linear relations. Both attacks try to recover the last round key. So the S-boxes are in particular designed to resist against the two cryptanalysis. Mathematically the functions that exhibit the best resistance against the differential attack are called *perfect nonlinear* [7]. The maximal level of security against the linear attack is provided by the *bent functions*, independently introduced by Dillon [3] and Rothaus [13]. In the Boolean setting, i.e., when considered functions are from $\mathsf{GF}(2)^m$ to $\mathsf{GF}(2)^n$ (with $\mathsf{GF}(2) = \{0, 1\}$), perfect nonlinearity and bentness are exactly the same notion, dual one from the other by the Fourier transform. This kind of functions was generalized by Logachev et al. [5] in order to treat the case of maps defined on a finite Abelian group and with values in the multiplicative group T of complex roots of the unity (in [9] is

[1] This generic name comes from its well-known homonyms used in the Data Encryption Standard [4].

considered a generalization for finite non-Abelian groups). In this contribution we develop a notion of bentness in order to treat the case of functions defined on an elementary finite Abelian p-group and with values in the multiplicative group $\mathsf{GF}(2^n)^*$ (with $p = 2^n - 1$) of roots of the unity of the finite field with 2^n elements $\mathsf{GF}(2^n)$, rather than in T. Like its classical version, this approach of bentness relies on a theory of characters of certain finite Abelian groups. But the characters, we introduce in this paper, are not T-valued but $\mathsf{GF}(2^n)^*$-valued. This *modulo* 2 *duality* allows us to define an appropriate *modulo* 2 *Fourier transform* on which is finally based the new concept of bentness called $\mathsf{GF}(2^n)$-*bentness*. In this paper we also construct some of these $\mathsf{GF}(2^n)$-bent functions and study their relations with perfect nonlinear functions. In particular we show that the (classical) notion of perfect nonlinearity is stronger (and not equivalent) than this new concept of bentness. However we also introduce a novel version of perfect nonlinearity which is shown equivalent to modulo 2 bentness.

Outline

The paper is divided in two parts. The first one is devoted to some classical results on bent and perfect nonlinear functions and in the second part, we present the generalized notion of bentness. More precisely in the following section are recalled some classical (and less classical) results on perfect nonlinear and bent functions. In particular we present a generalized notion of nonlinearity based on group actions that allows us to define additively and multiplicatively perfect nonlinear functions. Section 4 is devoted to the study of a particular function, called *finite field exponential*, which is proven to be multiplicatively (but not additively) perfect nonlinear. In fact this exponential is a particular instance of the new « modulo 2 » characters which are introduced in Section 5. Actually in Section 5, we develop a theory of $\mathsf{GF}(2^n)^*$-valued characters defined on an elementary finite Abelian p-group where $p = 2^n - 1$ is a Mersenne prime number. In Section 6 a relevant notion of Fourier transform, based on this modulo 2 duality, is introduced. Several of its properties - which generalize the traditional ones - are also presented. Finally in Section 7 we define the new concept of (modulo 2) bentness. In particular we construct such a function and we study the relations between these bent maps and classical (additively) and non-classical (group actions based) perfect nonlinearity.

Part I. Classical Notions

2. Perfect Nonlinear and Bent Functions

In this section, we briefly summarize some of the most relevant results of the mathematical topics of perfect nonlinearity and bentness. Most of the results presented in this part will be generalized in the characteristic 2 new setting we introduce in the second part.

2.1. Perfect nonlinear functions

In this contribution, 0 (resp., 1) is the neutral element of a group G written additively (resp., multiplicatively) and G^* is the subset of non-neutral elements of G. Nevertheless when $\mathbb{K}$ is a field, then $\mathbb{K}^*$ is the multiplicative group of nonzero elements in the field and the set of non-neutral elements of $\mathbb{K}^*$ is denoted by $\mathbb{K}^* \setminus \{1\}$ rather than using $\mathbb{K}^{**}$.

In its most generalized version [8, 10, 11], the notion of perfect nonlinearity is based on the concept of group action that we recall. Let G be a group and X be a nonempty set. We say that *G acts on X* if there is a group homomorphism $\phi : G \to S(X)$, where $S(X)$ is the group of bijective maps of X. Usually for $(g, x) \in G \times X$, we use the following convenient notation:

$$g \cdot x := \phi(g)(x) \tag{2}$$

and so we hide any explicit reference to the morphism ϕ. An action is called *faithful* if the corresponding homomorphism ϕ is one-to-one. It is called *regular* if for each $(x, y) \in X^2$ there is one and only one $g \in G$ such that $g \cdot x = y$. A regular action is also faithful.

Example 1.

- A group G acts on itself by translation: $g \cdot x := gx$ for $(g, x) \in G^2$ (G is here written multiplicatively). This action is regular;
- A subgroup H of a group G also acts on G by translation: $h \cdot x := hx$ for $(h, x) \in H \times G$. This action is faithful and if H is a proper subgroup, then the action is not regular;
- The multiplicative group $\mathbb{K}^*$ of a field $\mathbb{K}$ acts on $\mathbb{K}$ by the multiplication law of the group. This action is faithful but not regular since 0 is fixed by every elements of $\mathbb{K}^*$.

Let X and Y be two finite nonempty sets. A function f is called *balanced* if for each $y \in Y$,

$$|\{x \in X \mid f(x) = y\}| = \frac{|X|}{|Y|}, \tag{3}$$

where $|S|$ is the cardinality of a finite set S.

Using the concepts of group actions and balancedness, we can recall the definition of perfect nonlinear functions.

Definition 1. Let G be a finite group that acts faithfully on a finite nonempty set X. Let H be a finite group (written additively). A function $f : X \to H$ is called *perfect nonlinear* (with respect to the action of G on X) if for each $\alpha \in G^*$, the *derivative of f in direction* α,

$$\begin{aligned} d_\alpha f : X &\to H \\ x &\mapsto f(a \cdot x) - f(x) \end{aligned} \tag{4}$$

is balanced or in other words for each $\alpha \in G^*$ and each $\beta \in H$,

$$|\{x \in X \mid d_\alpha f(x) = \beta\}| = \frac{|X|}{|H|}. \tag{5}$$

This combinatorial notion is strictly equivalent to **classical** perfect nonlinear functions [2] when $X = G$ and the considered group action is the regular action of G on itself by translation. However in this generalized version, we can naturally introduce additively and multiplicatively perfect nonlinear functions on a finite field.

Definition 2. Let p be a prime number and $\mathsf{GF}(p^n)$ be the finite field with p^n elements. Let H be a finite group. A function $f : \mathsf{GF}(p^n) \to H$ is called

- *additively perfect nonlinear* if f is (classical) perfect nonlinear, i.e., for each $(\alpha, \beta) \in \mathsf{GF}(p^n)^* \times H$,

$$|\{x \in \mathsf{GF}(p^n) | f(\alpha + x) - f(x) = \beta\}| = \frac{|\mathsf{GF}(p^n)|}{|H|} = \frac{p^n}{|H|}; \qquad (6)$$

- *multiplicatively perfect nonlinear* if f is $\mathsf{GF}(p^n)^*$-perfect nonlinear, i.e., for each $(\alpha, \beta) \in (\mathsf{GF}(p^n)^* \setminus \{1\}) \times H$,

$$|\{x \in \mathsf{GF}(p^n) | f(\alpha x) - f(x) = \beta\}| = \frac{|\mathsf{GF}(p^n)|}{|H|}. \qquad (7)$$

In Section 4, a multiplicatively perfect nonlinear function is presented and in the last section of the paper, we deal with additively perfect nonlinear functions. Note also we will use the same notation for both additive and multiplicative derivatives (the context usually withdraws the doubts).

When we restrict to classical perfect nonlinear functions on finite Abelian groups, there is an equivalent characterization based on the Fourier transform and known under the name of *bent functions*. Such a characterization also exists for the general group action version [8, 11] and for finite non-Abelian groups [9]. But for the purpose of this paper we do not need to know the non-Abelian result.

2.2. Bent functions

The notion of bentness relies on the Fourier transform which is itself based on the theory of characters of finite Abelian groups. So we first recall these tools before introducing bent functions.

2.2.1. Theory of characters

Let G be a finite Abelian group (written additively). A *character of G* is a group homomorphism χ from G to the multiplicative group of complex roots of the unity $T := \{z \in \mathbb{C} \mid z\overline{z} = 1\}$ (where $\overline{z}$ is the complex modulus of $z \in \mathbb{C}$). In particular, $\chi(-x) = \overline{\chi(x)}$ and $\chi(0) = 1$. A character χ is called *trivial* if $\forall x \in G,\ \chi(x) = 1$ (or simply $\chi = 1$). The other characters are called *nontrivial* (and we use the notation $\chi \neq 1$ for such a nontrivial character). When equipped with the point-wise multiplication, the set $\hat{G}$ of all characters of G is a finite Abelian group isomorphic to G itself. $\hat{G}$ is called the *dual group* of G. The characters satisfy the well-known *orthogonality relation* which is generalized in Section 5 for the theory of characters with values in the multiplicative group $\mathsf{GF}(2^n)^*$ of roots of the unity in $\mathsf{GF}(2^n)$.

Proposition 1. *For each* $(\chi, \chi') \in \hat{G}^2$,

$$\sum_{x \in G} \chi(x)\overline{\chi'(x)} = \begin{cases} 0 & \textit{if } \chi \neq \chi' \\ |G| & \textit{if } \chi = \chi'. \end{cases} \tag{8}$$

If we consider the following *scalar product* of complex functions defined on G,

$$\langle f, g \rangle := \sum_{x \in G} f(x)\overline{g(x)}, \tag{9}$$

then the orthogonality relation exactly means that $\hat{G}$ is an orthogonal basis for the complex vector space $\mathbb{C}^G$. This property allows us to define the Fourier transform.

2.2.2. The Fourier transform

Let $f : G \to \mathbb{C}$. Then the *Fourier transform* of f is the function $\hat{f}$

defined by

$$\begin{aligned} \hat{f} : \hat{G} &\to \mathbb{C} \\ \chi &\mapsto \sum_{x \in G} f(x)\chi(x). \end{aligned} \tag{10}$$

So the Fourier transform of f is exactly the decomposition of f in the basis of characters.

In this short subsection, we present a list of some of the classical properties of the Fourier transform that in particular are generalized in Section 6.

The Fourier transform is an invertible function and we have the following *inversion formula*:

$$f(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\overline{\chi(x)}. \tag{11}$$

We define the *convolutional product* of two complex-valued functions defined on G by the function $f * g$,

$$\begin{aligned} f * g : G &\to \mathbb{C} \\ \alpha &\mapsto (f * g)(\alpha) := \sum_{x \in G} f(x)g(-x + \alpha). \end{aligned} \tag{12}$$

Then the Fourier transform trivializes this convolutional product to a point-wise product. Indeed for each $\chi \in \hat{G}$,

$$(\widehat{f * g})(\chi) = \hat{f}(\chi)\hat{g}(\chi). \tag{13}$$

Using this trivialization it is possible to prove the following result.

Proposition 2. *Let f and g be two complex-valued functions defined on G. Then the Plancherel formula holds*

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\overline{\hat{g}(\chi)} = \sum_{x \in G} f(x)\overline{g(x)}. \tag{14}$$

Moreover if $g = f$, *we obtain the Parseval formula*

$$\frac{1}{|G|}\sum_{\chi\in\hat{G}}|\hat{f}(\chi)|^2 = \sum_{x\in G}|f(x)|^2, \tag{15}$$

where $|z|^2 = z\bar{z}$ *is the complex modulus of* $z \in \mathbb{C}$.

Finally if f is T-valued, the Parseval formula becomes

$$\sum_{\chi\in\hat{G}}|\hat{f}(\chi)|^2 = |G|^2. \tag{16}$$

In Sections 5 and 6, we generalize the theory of characters and the Fourier transform to deal with function defined on an elementary finite Abelian p-group and with values in the unit circle of the finite field $\mathsf{GF}(p+1)$, rather than in the complex roots of the unity T. We use the same notations (but they will be clear from the context) and we prove that the above properties also hold in the new context.

Now let us introduce the traditional concept of bentness which is also generalized in Section 7.

2.2.3. Bent functions

Bent functions were introduced independently and rather simultaneously by Dillon [3] and Rothaus [13]. Several years after, Logachev, Salnikov and Yashchenko presented a generalization of this concept in [5].

Definition 3. Let G be a finite Abelian group. A function $f : G \to T$ is called *bent* (*in the sense of Logachev*, *Salnikov and Yashchenko*) if for each $\chi \in \hat{G}$,

$$|\hat{f}(\chi)|^2 = |G|. \tag{17}$$

Note that in [9] this notion has been generalized to the case of finite non-Abelian groups but this is not relevant for the purpose of this paper.

As in the finite group setting, we can introduce a *derivative* for a function $f : G \to T$ which is defined for $\alpha \in G$ by

$$
\begin{aligned}
d_\alpha f : G &\to T \\
x &\mapsto f(\alpha + x)\overline{f(x)}.
\end{aligned}
\tag{18}
$$

Then Logachev, Salnikov and Yashchenko proved the following (see [5]).

Proposition 3. *A function $f : G \to T$ is bent if and only if for each $\alpha \in G^*$,*

$$\sum_{x \in G} d_\alpha f(x) = 0. \tag{19}$$

This is the masterpiece to prove the equivalence between bent and perfect nonlinear functions in finite Abelian groups as we will see soon.

Definition 4. Let G and H be two finite Abelian groups. A function $f : G \to H$ is called *bent* if for each nontrivial character $\chi' \in \hat{H}$, the map $\chi' \circ f : G \to T$ is bent in the sense of Logachev, Salnikov and Yashchenko.

Then using the proposition above, Carlet and Ding in [2] and Pott in [12] prove that bentness and perfect nonlinearity are equivalent in the finite Abelian groups setting[2].

Theorem 1. *Let G and H be two finite Abelian groups. Then a function $f : G \to H$ is (classical) perfect nonlinear if and only if f is bent.*

In [8, 11] is given a characterization of perfect nonlinearity with respect to a group action in terms of the Fourier transform quite similar to the previous theorem.

Theorem 2. *Let G be a finite Abelian group that acts faithfully on a finite nonempty set X. Let H be a finite Abelian group. A function $f : X \to H$ is perfect nonlinear (with respect to the group action of G on*

[2] In [9] this equivalence is generalized to the finite non-Abelian groups framework.

X) *if and only if for each nontrivial character* χ *of H and for each* $\alpha \in G$,

$$\frac{1}{|X|}\sum_{x\in X}|\,(\widehat{\chi \circ f_x})(\alpha)\,|^2 = |\,G\,|, \tag{20}$$

where for each $x \in X$ *we define*

$$\begin{aligned} f_x &: G \to H \\ &\alpha \mapsto f(\alpha \cdot x). \end{aligned} \tag{21}$$

Roughly speaking, a function is perfect nonlinear with respect to a group action if and only if the sequence of functions f_x is bent in average over all $x \in X$.

In Section 7 we introduce a new bentness notion and we show that up to a natural change in the definition of perfect nonlinearity, both previous theorems remain valid in the new setting.

2.3. Perfect nonlinearity and difference sets

The notion of perfect nonlinearity can be related to some combinatorics objects called (*relative*) *difference sets*.

Definition 5. Let *G* be any finite group that acts faithfully on a finite nonempty set *X* of cardinality *v*. Let *H* be a finite group of cardinality *m*. We define the faitful action of $G \times H$ on $X \times H$ by $(g, h)\cdot(x, h') :=$ $(g \cdot x, h + h')$ for $(x, g, h, h') \in X \times G \times H \times H$, i.e., it is the action of *G* on *X* on the first component and the regular action of *H* on the second component. Let $R \subset X \times H$ of cardinality *k*. *R* is called a $G \times H$-$(v, m\ k, \lambda)$*-difference set of* $X \times H$ *relative to* $\{0\} \times H$ if

(1) for every $(g, h) \neq (0, h) \in G \times H$, there are exactly λ solutions $((x_1, h_1), (x_2, h_2)) \in R^2$ such that $(g, h)\cdot(x_1, h_1) = (x_2, h_2)$;

(2) if (x, h) and (x, h') belong to *R*, then $h = h'$.

Such a $G\times H$-(v, m, k, λ)-relative difference set is called *semiregular* if $v = k$.

Note that each $G \times H$ -semiregular relative difference set R gives rise to a function $f : X \to H$ such that $R = \{(x, f(x)) | x \in X\}$.

The definition above is a generalization of classical relative difference sets for which $X = G$ and the action of G on X is simply the regular action of G on itself by translation (see for instance [12]).

Theorem 3. *Let G be any finite group that acts faithfully on a finite nonempty set X of cardinality v. Let H be a finite group of cardinality m. Then a function $f : X \to H$ is perfect nonlinear (with respect to the action of G on X) if and only if $R := \{(x, f(x)) | x \in X\}$ is a semiregular $G \times H$ -difference set of $X \times H$ relative to $\{0\} \times H$ with $\lambda = \frac{v}{m}$.*

Proof. Since f is a mapping, $| R | = | G |$ and therefore we need to prove that f is G-perfect nonlinear if and only if R satisfies axiom (ii) of $G \times H$ -relative difference sets with $\lambda = \frac{| X |}{| H |} = \frac{v}{m}$. This last assertion is equivalent to the following ones for each $(g, h) \in G^* \times H$,

$$| \{((x_1, h_1), (x_2, h_2)) \in R^2 | (g, h) \cdot (x_1, h_1) = (x_2, h_2)\} | = \frac{| X |}{| H |}$$

$$\Leftrightarrow | \{((x_1, h_1), (x_2, h_2)) \in R^2 | (g \cdot x_1, h + f(x_1)) = (x_2, f(x_2))\} | = \frac{| X |}{| H |}$$

(by the definition of the action of $G \times H$ on $X \times H$ and the definition of R)

$$\Leftrightarrow | \{x \in X | f(g \cdot x) - f(x) = h\} | = \left| \frac{X}{H} \right|$$

$\Leftrightarrow$ f is perfect nonlinear (with respect to the action of G on X).

This is a generalization of the equivalence between classical relative difference sets and classical perfect nonlinear functions (see [12]). We will generalize this result to the modulo 2 framework.

Part II. $\mathsf{GF}(2^n)^*$-bent Functions and their Properties

3. Introduction

This second part is devoted to the presentation of a new notion of bentness in order to treat the case of functions defined on an elementary finite Abelian p-group G and with values in $\mathsf{GF}(2^n)^*$ (with $p = 2^n - 1$). In the classical theory of bent functions, such a map f is bent if for each nontrivial character of $\mathsf{GF}(2^n)^*$, the function $\chi \circ f : G \to T$ is bent in the sense of Logachev, Salnikov and Yashchenko or equivalently, f is (classical) perfect nonlinear. In our own approach we directly adapt the notion of bent functions of Logachev, Salnikov and Yashchenko to the case of $\mathsf{GF}(2^n)^*$-valued functions, without using any complex-valued characters. More precisely we introduce a nonusual theory of characters for G since we consider as characters the group homomorphisms from G to the roots of the unity $\mathsf{GF}(2^n)^*$ rather than T-valued characters. In short we replace the complex field $\mathbb{C}$ by a finite field $\mathsf{GF}(2^n)$. This notion of *modulo* 2 (or *characteristic* 2) characters satisfies some relevant properties (such as an orthogonality relation for the characters) which enables us to construct an interesting modulo 2 Fourier transform that deals with $\mathsf{GF}(2^n)$-valued functions rather than $\mathbb{C}$-valued functions for its classical counterpart. Using this modular version of the Fourier transform, we introduce an appropriate notion of bent functions which are exactly the characteristic 2 equivalents to the bent functions of Logachev, Salnikov and Yashchenko. Finally we study the relations between classical perfect nonlinearity and modulo 2 bentness. In particular we show that the second one is a weaker notion than the first one. However we also introduce a weaker notion of perfect nonlinearity which is proven equivalent to the new modulo 2 bentness notion.

4. Finite Field Exponential Function

In this section we define an exponential-like function in the finite field setting. In particular such a function should be a group isomorphism from $\mathsf{GF}(p^m)$ to $\mathsf{GF}(q^n)^*$, where p and q are two prime numbers such that $p^m = q^n - 1$. Since $\mathsf{GF}(q^n)^*$ is a cyclic group of order $q^n - 1$, m must be equal to 1 (because $\mathsf{GF}(p)$ is the only finite field with a cyclic additive group). Therefore we need to find a pair of prime integers (p, q) and a nonzero natural number n such that $p = q^n - 1$. Moreover if q is an odd prime number, q^n is also odd for each nonzero n, so $q^n - 1$ is an even integer and then $p = 2$ (in this case $q = 3$ and $n = 1$). For an odd prime number p, we need to choose $q = 2$. For the remainder of the paper, we consider an odd prime number p so that $p = 2^m - 1$. We have for instance $3 = 2^2 - 1, 7 = 2^4 - 1, 31 = 2^5 - 1, \ldots, 2^{61} - 1, \ldots, 2^{32582657} - 1$. Such numbers are called *Mersenne prime numbers*. Note that if $p = 2^n - 1$, then $\mathsf{GF}(p)$ and $\mathsf{GF}(2^n)^*$ are isomorphic. In the remainder of this paper the prime finite field $\mathsf{GF}(p)$ is interpreted as $\{0, 1, \ldots, p - 1\}$.

So let given a Mersenne prime number $p = 2^n - 1$. Now let $\gamma \in \mathsf{GF}(2^n)^*$ be a primitive root of the unity. We define the function

$$\begin{aligned} e_\gamma : \mathsf{GF}(p) &\to \mathsf{GF}(2^n)^* \\ k &\mapsto \gamma^k. \end{aligned} \tag{22}$$

Then e_γ is obviously a group isomorphism from $\mathsf{GF}(p)$ to $\mathsf{GF}(2^n)^*$. This function is an exponential-like mapping because the following equalities hold:

1. $e_\gamma(0) = 1$;

2. $e_\gamma(k + k') = \gamma^{k+k'} = \gamma^k\gamma^{k'} = e_\gamma(k)e_\gamma(k')$;

3. $e_\gamma(-k) = \gamma^{-k} = (e_\gamma(k))^{-1}$;

4. $e_\gamma(kk') = \gamma^{kk'} = (\gamma^k)^{k'} = (e_\gamma(k))^{k'}$.

The inverse isomorphism of e_γ is denoted by l_γ and acts as a logarithm function because $l_\gamma(1) = 0$, $l_\gamma(kk') = l_\gamma(k) + l_\gamma(k')$. The exponential function has an interesting cryptographic property.

Theorem 4. *The exponential function* e_γ *is a multiplicatively perfect nonlinear permutation.*

Proof. Let $(\alpha, \beta) \in \mathsf{GF}(p)^* \setminus \{1\} \times \mathsf{GF}(2^n)^*$. We need to show that there is one and only one element $x \in GF(p)$ such that $d_\alpha e_\gamma(x) := \dfrac{e_\gamma(\alpha x)}{e_\gamma(x)} = \beta$,

$$\frac{e_\gamma(\alpha x)}{e_\gamma(x)} = \beta$$

$$\Leftrightarrow e_\gamma(\alpha x - x) = \beta$$

$$\Leftrightarrow (\alpha - 1)x = l_\gamma(\beta)$$

$$\Leftrightarrow x = \frac{1}{\alpha - 1} l_\gamma(\beta)\ (\alpha \neq 1). \tag{23}$$

Note that e_γ is not additively perfect nonlinear. Indeed let $(\alpha, \beta) \in \mathsf{GF}(p)^* \times \mathsf{GF}(2^n)$. Let us suppose that $\beta \neq 0$. Let us compute the number of solutions $x \in \mathsf{GF}(p)$ to the equation $d_\alpha e_\gamma(x) := e_\gamma(\alpha + x) - e_\gamma(x) = \beta$,

$$e_\gamma(\alpha + x) - e_\gamma(x) = \beta$$

$$\Leftrightarrow e_\gamma(\alpha)e_\gamma(x) - e_\gamma(x) = \beta$$

$$\Leftrightarrow (e_\gamma(\alpha) - 1)e_\gamma(x) = \beta$$

$$\Leftrightarrow e_\gamma(x) = \frac{1}{e_\gamma(\alpha) - 1}\beta\ \text{(because } \alpha \neq 0)$$

$$\Leftrightarrow x = \ln\left(\frac{1}{e_\gamma(\alpha) - 1}\beta\right) = -\ln(e_\gamma(\alpha - 1)) + \ln(\beta) = 1 - \alpha + \ln(\beta). \tag{24}$$

But now if $\beta = 0$, then we have

$$\begin{aligned} & e_\gamma(\alpha + x) = e_\gamma(x) \\ \Leftrightarrow\ & \alpha + x = x \\ \Leftrightarrow\ & \alpha = 0 \end{aligned} \tag{25}$$

which is a contradiction. In fact e_γ could be called *almost additively perfect nonlinear* since for each $\alpha \in \mathsf{GF}(p)^*$ and each $\beta \in \mathsf{GF}(2^n)$,

$$|\{x \in \mathsf{GF}(p) | e_\gamma(\alpha + x) - e_\gamma(x) = \beta\}| \in \{0, 1\}.$$

This exponential function can also be seen as a particular *character* of $\mathsf{GF}(p)$ not valued in the multiplicative group of complex roots of the unity T but in $\mathsf{GF}(2^n)^*$. We introduce such a finite field version of finite group duality in next section.

5. Finite Abelian Group Duality in Characteristic 2

From now on, we suppose given a Mersenne prime number: $p = 2^n - 1$ and $G := \mathsf{GF}(p)^m$.

Definition 6. A $\mathsf{GF}(2^n)$*-character* of G is a group homomorphism from (the additive group) G to $\mathsf{GF}(2^n)^*$.

Note that this definition remains valid if we consider any finite elementary Abelian p-group for G since we only use the additive structure of G (and not the multiplicative structure of the field $\mathsf{GF}(p)$).

The exponential function e_γ is a $\mathsf{GF}(2^n)$-character of $\mathsf{GF}(p)$. Let χ be a $\mathsf{GF}(2^n)$-character of G. For each $x \in G$, we have $\chi(-x) = (\chi(x))^{-1} = (\chi(x))^{2^n-2}$ and $\chi(0) = 1$. The set of all $\mathsf{GF}(2^n)$-characters of G is denoted by $\hat{G}$ (as its classical counterpart). When equipped with the point-wise multiplication, defined for $(\chi, \chi') \in \hat{G}^2$ by

$$\chi\chi' : x \mapsto \chi(x)\chi'(x), \tag{26}$$

$\hat{G}$ is a finite Abelian group which is called the $\mathsf{GF}(2^n)$-*dual group* of G. We can even prove a better result.

Theorem 5. $\widehat{\mathsf{GF}(p)}$ *and* $\mathsf{GF}(p)$ *are isomorphic.*

Proof. Let γ be a primitive root of $\mathsf{GF}(2^n)$. Then we show that the elements of $\widehat{\mathsf{GF}(2^n)}$ have the following form, for $j \in \mathsf{GF}(p)$,

$$\begin{aligned} \chi_j : \mathsf{GF}(p) &\to \mathsf{GF}(2^n) \\ k &\mapsto (\gamma^j)^k. \end{aligned} \tag{27}$$

Let $\chi \in \widehat{\mathsf{GF}(p)}$. In order to determine it, we must compute the value $\chi(k) = \chi(k1) = \chi(\underbrace{1 + \cdots + 1}_{k \text{ times}}) = (\chi(1))^k$ for $k \in \mathsf{GF}(p)$. So we have $\chi(k) = \gamma^{jk}$, where $\chi(1) = \gamma^j$ for one $j \in \mathsf{GF}(p)$ since $\chi(1) \in \mathsf{GF}(2^n)^*$. Then χ is a element of $\{\chi_0, \ldots, \chi_{p-1}\}$. Reciprocally, we note that for $j \in \mathsf{GF}(p)$, the functions χ_j are group homomorphisms from $\mathsf{GF}(p)$ to $\mathsf{GF}(2^n)^*$, so they are elements of $\widehat{\mathsf{GF}(p)}$. Let define the following map:

$$\begin{aligned} \Psi : \mathsf{GF}(p) &\to \widehat{\mathsf{GF}(p)} \\ j &\mapsto \chi_j. \end{aligned} \tag{28}$$

We already know that Ψ is onto. Moreover Ψ is also one-to-one ($\Psi(i) = \Psi(j)$ if and only if for all $k \in \mathsf{GF}(p)$, $\gamma^{ik} = \gamma^{jk}$, so in particular $\gamma^i = \gamma^j$ which implies that $i = j$). Since Ψ is also a group homomorphism, we deduce that $\widehat{\mathsf{GF}(p)}$ and $\mathsf{GF}(p)$ are isomorphic.

Note 1. If $C_p := \langle g \rangle = \{g^k \mid k \in \{0, ..., p-1\}\}$ is a cyclic group of order p, then we also have the fact that C_p and $\widehat{C_p}$ are isomorphic and the character associated to g^k is simply the map χ_{g^k} defined by

$$\begin{aligned} \chi_{g^k} : C_p &\to \mathsf{GF}(2^n)^* \\ g^k &\mapsto (\gamma^j)^k. \end{aligned} \tag{29}$$

Theorem 6. $\mathsf{GF}(p)^2$ *and* $\widehat{\mathsf{GF}(p)^2}$ *are isomorphic.*

Proof. It is sufficient to show that $\widehat{\mathsf{GF}(p)^2}$ and $\widehat{\mathsf{GF}(p)} \times \widehat{\mathsf{GF}(p)}$ are isomorphic. Let i_1 be the first canonical injection of $\mathsf{GF}(p) \times \mathsf{GF}(p)$ and i_2 be the second one. The function

$$\begin{aligned} \Phi : \widehat{\mathsf{GF}(p)^2} &\to \widehat{\mathsf{GF}(p)} \times \widehat{\mathsf{GF}(p)} \\ \chi &\mapsto (\chi \circ i_1, \chi \circ i_2) \end{aligned} \tag{30}$$

is a group homomorphism. It is obviously one-to-one and for $(\chi', \chi'') \in \widehat{\mathsf{GF}(p)} \times \widehat{\mathsf{GF}(p)}$, the map $\chi : (x, y) \mapsto \chi'(x)\chi''(y)$ is an element of $\widehat{\mathsf{GF}(p)^2}$ and $\Phi(\chi) = (\chi', \chi'')$. So $\widehat{\mathsf{GF}(p)^2}$ is isomorphic to $\widehat{\mathsf{GF}(p)} \times \widehat{\mathsf{GF}(p)}$ which is itself isomorphic to $\mathsf{GF}(p)^2$.

By iteration we find that $\widehat{\mathsf{GF}(p)^m}$ and $\mathsf{GF}(p)^m$ are isomorphic[3]. Using the natural dot-product[4] over $\mathsf{GF}(p)^m$, which is defined for

[3] More generally if G is an elementary finite Abelian p-group, then G is isomorphic to $\hat{G}$.

[4] For a direct product C_p^m, where $C_p = \langle g \rangle$, one can also define a dot-product by $(g^{i_1}, ..., g^{i_m}) \cdot (g^{j_1}, ..., g^{j_n}) := \sum_{k=1}^{m} i_k j_k \in \mathsf{GF}(p)$. But this is not a canonical dot-product since it depends on the generator g.

$(x, y) \in (\mathsf{GF}(p)^m)^2$ by

$$x \cdot y := \sum_{i=1}^{m} x_i y_i \in \mathsf{GF}(p) \tag{31}$$

we can give an explicit form for a character[5] of $\mathsf{GF}(p)^m$. Let $\alpha \in \mathsf{GF}(p)^m$. Then the character[6] corresponding to α is given by

$$\begin{aligned} \chi_\alpha : \mathsf{GF}(p)^m &\to \mathsf{GF}(2^n)^* \\ x &\mapsto \gamma^{\alpha \cdot x}. \end{aligned} \tag{32}$$

In particular $\chi_\alpha(x) = \chi_x(\alpha)$ for each $(\alpha, x) \in (\mathsf{GF}(p)^m)^2$. Note that if G is any elementary finite Abelian p-group, this equality also holds. Indeed such a group is isomorphic to a certain direct product C_p^m, where C_p is a cyclic group of order p (we denote by Φ the isomorphism). The characters of this direct product have the form $\chi_\alpha(x) := \gamma^{\alpha \cdot x}$, where $(\alpha, x) \in (C_p^m)^2$. Then the characters of G have the form $\chi'_\alpha(x) := \chi_{\Phi(\alpha)}(\Phi(x))$, where $(\alpha, x) \in G^2$. Finally $\chi'_\alpha(x) = \chi'_x(\alpha)$.

From now on, we suppose that G is an elementary finite Abelian p-group (written additively). We denote by χ_α the character of G associated to $\alpha \in G$ by a (fixed) group isomorphism from G to $\hat{G}$.

Lemma 1. *For $\chi \in \hat{G}$, we have*

$$\sum_{x \in G} \chi(x) = \begin{cases} 0 & \text{if } \chi \neq 1, \\ |\,G\,| \pmod 2 = 1 & \text{if } \chi = 1. \end{cases} \tag{33}$$

[5] If we consider the case of an elementary finite Abelian p-group there is no such canonical description of the characters because there is no natural dot-product.

[6] When is fixed a generator, we can do exactly the same for C_p^m.

Proof. If $\chi = 1$, then $\sum_{x \in G} 1 = |G| \pmod 2 = p^m \pmod 2 = 1$ (since we count in characteristic 2 and G is isomorphic to a certain direct product C_p^m and the product of odd integers is an odd integer). Now let us suppose that $\chi \neq 1$. Let $x_0 \in G$ such that $\chi(x_0) \neq 1$. Then we have $\chi(x_0) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(x_0 + x) = \sum_{x \in G} \chi(x)$. Therefore $(\chi(x_0) - 1) \sum_{x \in G} \chi(x) = 0$ and since $\chi(x_0) \neq 1$, $\sum_{x \in G} \chi(x) = 0$.

Definition 7. Now let us define the analogue to the conjugate in this setting. Let $z \in \mathsf{GF}(2^n)$,

$$\overline{z} := z^{2^n - 2} = \begin{cases} 0 & \text{if } z = 0, \\ z^{-1} & \text{if } z \in \mathsf{GF}(2^n)^*. \end{cases}$$

We call this the *conjugate* of *z*. This is an abuse of language because even if like the complex conjugate, $\overline{zz'} = \overline{z}\overline{z'}$ and $z\overline{z} = 1$ (for $z \neq 0$), contrary to the complex conjugate, this version is not linear with respect to + (unless for instance for $n = 2$, since $2^2 - 2 = 2$ and $x \mapsto x^2$ is linear in $\mathsf{GF}(4)$ or more generally if there is $0 < k < n$ such that $2^n - 2 = 2^k$ which is equivalent to $2^k(2^{n-k} - 1) = 2$. But $2^k \underbrace{(2^{n-k} - 1)}_{\geq 1} \geq 2^k \geq 2$ and with equality in the last inequality if and only if $k = 1$ and in the first inequality if $n = k + 1 = 2$ which is exactly the previous case). Moreover we define a *scalar product* for functions defined on G and with values in $\mathsf{GF}(2^n)$: let *f* and *g* be two such functions. Their « *scalar product* » is then naturally defined by

$$\langle f, g \rangle := \sum_{x \in G} f(x)\overline{g(x)} \in \mathsf{GF}(2^n). \tag{34}$$

Let us see some properties of this object. Let $(f, g, h) \in (\mathsf{GF}(2^n)^G)^3$ and $\alpha \in \mathsf{GF}(2^n)$. It is obvious to check that $\langle f + g, h \rangle = \langle f, h \rangle + \langle g, h \rangle$,

$\langle \alpha f, g\rangle = \alpha\langle f, g\rangle$ and $\langle f, \alpha g\rangle = \overline{\alpha}\langle f, g\rangle$. But the map $g \mapsto \langle f, g\rangle$ with a fixed f is generally not linear (this is due to the fact that $x \mapsto \overline{x}$ is generally not linear itself) nor the map $(f, g) \mapsto \langle f, g\rangle$ is conjugate symmetric (we can prove that $\langle f, g\rangle = \langle \overline{g}, \overline{f}\rangle$ which may differ from $\overline{\langle g, f\rangle}$ since another time $x \mapsto \overline{x}$ can be nonlinear). Nevertheless we can prove that $\langle .,.\rangle$ is a kind of nondegenerate in the sense that $\langle f, g\rangle = 0$ for all g if and only if f is uniformly equal to 0 (to see this, it is sufficient to compute $\langle f, \delta_{x_0}\rangle = f(x_0) = 0$ for each $x_0 \in G$ and where δ_{x_0} is the Dirac mass centered in x_0 and defined by $\delta_{x_0}(x) = \begin{cases} 0 & \text{if } x \neq x_0 \\ 1 & \text{if } x = x_0 \end{cases}$). Note also that the skew *norm* $\| f \| := \langle f, f\rangle$ satisfies the *positive homogeneity*, since for each $\alpha \in \mathsf{GF}(2^n)$, $\| \alpha f \| = | \alpha | \|f\|$, where we define

$$| \alpha | := \alpha\overline{\alpha} = \begin{cases} 0 & \text{if } \alpha = 0, \\ 1 & \text{if } \alpha \in \mathsf{GF}(2^n)^* \end{cases} \tag{35}$$

but *positive definiteness* does not hold, i.e., we can find $f : G \to \mathsf{GF}(2^n)$ such that f is non-uniformally null but $\| f \| = 0$. Indeed let f be such that its *support* $S(f) := \{x \in G \,|\, f(x) \neq 0\}$ has an even (and nonzero) number of elements. Then $\| f \| = | S(f) | (\operatorname{mod} 2) = 0$.

Nevertheless with this *skew* scalar product and Lemma 1 above, we can show that the $\mathsf{GF}(2^n)$-characters satisfy a kind of orthogonality (even orthonormality) relation (similar to the one of the complex-valued characters case).

Corollary 1. *For each* $(\chi', \chi'') \in \hat{G}^2$ *we have*

$$\langle \chi', \chi''\rangle = \begin{cases} 0 & \textit{if } \chi' \neq \chi'', \\ 1 & \textit{if } \chi' = \chi''. \end{cases} \tag{36}$$

Proof. Let $\chi := \chi'(\chi'')^{-1} = \chi'\overline{\chi''}$. Then $\langle \chi', \chi''\rangle = \sum\limits_{x \in G} \chi(x)$. If $\chi' = \chi''$, then $\chi = 1$ and if $\chi' \neq \chi''$, then $\chi \neq 1$. Using the previous Lemma 1, we conclude the proof.

Informally speaking the $\mathsf{GF}(2^n)$-characters of G form some skew type of orthonormal basis of the $\mathsf{GF}(2^n)$-vector space $\mathsf{GF}(2^n)^G$. This is exactly what we need to construct a Fourier transform with good properties.

6. Characteristic 2 Fourier Transform and its Properties

Let $f : G \to \mathsf{GF}(2^n)$. We define its Fourier transform by

$$\begin{aligned} \hat{f} : \hat{G} &\to \mathsf{GF}(2^n) \\ \chi &\mapsto \sum_{x \in G} f(x)\chi(x). \end{aligned} \tag{37}$$

In particular due to the isomorphism from $\hat{G}$ onto G, we have actually

$$\begin{aligned} \hat{f} : G &\to \mathsf{GF}(2^n) \\ \alpha &\mapsto \hat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x). \end{aligned} \tag{38}$$

In particular if $G = \mathsf{GF}(p)^m$, then $\hat{f}(\alpha) = \sum_{x \in G} f(x)\gamma^{\alpha \cdot x}$.

Let us compute $\hat{\hat{f}}$. Let $\alpha \in G$,

$$\begin{aligned} \hat{\hat{f}}(\alpha) &= \sum_{x \in G} \hat{f}(x)\chi_\alpha(x) \\ &= \sum_{x \in G} \sum_{y \in G} f(y)\chi_x(y)\chi_\alpha(x) \\ &= \sum_{x \in G} \sum_{y \in G} f(y)\chi_y(x)\chi_\alpha(x) \quad \text{(since } \chi_x(y) = \chi_y(x)\text{)} \end{aligned}$$

$$= \sum_{y \in G} f(y) \underbrace{\sum_{x \in G} \chi_{\alpha+y}(x)}_{= \begin{cases} 0 & \text{if } -\alpha \neq y, \\ 1 & \text{if } -\alpha = y. \end{cases}}$$

$$= f(-\alpha). \tag{39}$$

Then we have the *inversion formula*

$$f(x) = \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)}. \tag{40}$$

Definition 8. Let $(f, g) \in (\mathsf{GF}(2^n)^G)^2$. Then we define the *convolutional product* of f and g by

$$f * g : G \to \mathsf{GF}(2^n)$$

$$\alpha \mapsto (f * g)(\alpha) := \sum_{x \in G} f(x) g(-x + \alpha). \tag{41}$$

Proposition 4. *Let* $(f, g) \in (\mathsf{GF}(2^n)^G)^2$. *For each* $\alpha \in G$, *we have*

$$\widehat{(f * g)}(\alpha) = \hat{f}(\alpha)\hat{g}(\alpha). \tag{42}$$

Proof. Let $\alpha \in G$. The following sequence of equalities holds:

$$\widehat{(f * g)}(\alpha) = \sum_{x \in G} (f * g)(x)\chi_\alpha(x)$$

$$= \sum_{x \in G} \sum_{y \in G} f(y) g(-y + x)\chi_\alpha(x)$$

$$= \sum_{x \in G} \sum_{y \in G} f(y) g(-y + x)\chi_\alpha(y - y + x)$$

$$= \sum_{x \in G} \sum_{y \in G} f(y) g(-y + x)\chi_\alpha(y)\chi_\alpha(-y + x)$$

$$= \sum_{y \in G} f(y)\chi_\alpha(y) \sum_{x \in G} g(-y+x)\chi_\alpha(-y+x)$$

$$= \hat{f}(\alpha)\hat{g}(\alpha). \tag{43}$$

Theorem 7 (Plancherel formula)**.** *Let* $(f, g) \in (\mathsf{GF}(2^n)^G)^2$. *Then we have*

$$\sum_{x \in G} f(x)\overline{g(x)} = \sum_{\alpha \in G} \hat{f}(\alpha)\hat{\overline{g}}(-\alpha). \tag{44}$$

Proof. For any function h from G to $\mathsf{GF}(2^n)$ the following map is defined:

$$\overline{h} : G \to \mathsf{GF}(2^n)$$

$$x \mapsto \overline{h(x)}. \tag{45}$$

We also define the *function* $i_G : x \in G \mapsto -x \in G$. Then one has

$$(f * \overline{g} \circ i_G)(0) = \sum_{x \in G} f(x)\overline{g}(i_G(-x+0)) = \sum_{x \in G} f(x)\overline{g(x)}. \tag{46}$$

According to the inversion formula, we also have

$$(f * \overline{g} \circ i_G)(0) = \sum_{\alpha \in G} (\widehat{f * \overline{g} \circ i_G})(\alpha)$$

$$= \sum_{\alpha \in G} \hat{f}(\alpha)(\widehat{\overline{g} \circ i_G})(\alpha) \text{ (according to Proposition 4).} \tag{47}$$

Let us compute $(\widehat{\overline{g} \circ i_G})(\alpha)$.

$$(\widehat{\overline{g} \circ i_G})(\alpha) = \sum_{x \in G} (\overline{g} \circ i_G)(x)\chi_\alpha(x)$$

$$= \sum_{x \in G} \overline{g(-x)}\chi_\alpha(x)$$

$$= \sum_{x \in G} \overline{g(x)} \chi_\alpha(-x)$$

$$= \sum_{x \in G} \overline{g(x)} \overline{\chi_\alpha(x)}$$

$$= \sum_{x \in G} \overline{g(x)} \chi_{-\alpha}(x)$$

$$= \hat{\hat{g}}(-\alpha). \tag{48}$$

Note that this version of the Plancherel formula is not identical to the traditional one. This is essentially due to the fact that $\overline{z_1 + z_2} \neq \overline{z_1} + \overline{z_2}$ for some $(z_1, z_2) \in (\mathsf{GF}(2^n))^2$, so in particular $(\widehat{\overline{g} \circ i_G})(\alpha) \neq \overline{\hat{g}(\alpha)}$.

Corollary 2 (Parseval relation)**.** *Let* $f : G \to \mathsf{GF}(2^n)$. *Then we have*

$$| S(f) | (\text{mod } 2) = \sum_{\alpha \in G} \hat{f}(\alpha) \hat{\hat{f}}(-\alpha), \tag{49}$$

where $S(f) := \{x \in G \,|\, f(x) \neq 0\}$ *is the support of f.*

In particular if f is $\mathsf{GF}(2^n)^*$*-valued, then*

$$\sum_{\alpha \in G} \hat{f}(\alpha) \hat{\hat{f}}(-\alpha) = 1. \tag{50}$$

Proof. The first equality is obtained by applying Plancherel formula with $g = f$. Since $\overline{f(x)} = (f(x))^{-1}$ when $f(x) \neq 0$ and 0 otherwise,

$$\sum_{x \in G} f(x) \overline{f(x)} = \sum_{x \in G \text{ such that } f(x) \neq 0} 1 = | \{x \in G \,|\, f(x) \neq 0\} | (\text{mod } 2).$$

The second equality obviously holds since $S(f) = G$ and $| G | (\text{mod } 2) = 1$.

Regarding the classical Parseval relation recall Section 2, we note in particular that $\hat{f}(\alpha) \hat{\hat{f}}(-\alpha)$ plays the role of $| \hat{f}(\alpha) |^2$ in the classical setting. This remark is essential for the definition of the new bentness notion.

7. Characteristic 2 Bent Functions and Perfect Nonlinearity

7.1. $\mathsf{GF}(2^n)$-bentness

Definition 9. A function $f : G \to \mathsf{GF}(2^n)^*$ is called $\mathsf{GF}(2^n)$-*bent* (or simply *bent*) if for all $\alpha \in G$,

$$\hat{f}(\alpha)\hat{\bar{f}}(-\alpha) = 1. \tag{51}$$

Proposition 5. *If the function* $f : G \to \mathsf{GF}(2^n)^*$ *is* $\mathsf{GF}(2^n)$-*bent, then for each* $\beta \in \mathsf{GF}(2^n)^*$, *the function*

$$\begin{aligned} \beta f : G &\to \mathsf{GF}(2^n)^* \\ x &\mapsto \beta f(x) \end{aligned} \tag{52}$$

is also $\mathsf{GF}(2^n)$-*bent.*

Proof. Let us compute

$$\widehat{\beta f}(\alpha) = \sum_{x\in G} \beta f(x)\chi_\alpha(x) = \beta \sum_{x\in G} f(x)\chi_\alpha(x) = \beta\hat{f}(\alpha).$$

Now let us compute

$$\widehat{\overline{\beta f}}(-\alpha) = \sum_{x\in G} \overline{\beta f(x)}\chi_{-\alpha}(x) = \bar{\beta}\sum_{x\in G} \overline{f(x)}\chi_{-\alpha}(x) = \bar{\beta}\hat{\bar{f}}(-\alpha).$$

So we have $\widehat{\beta f}(\alpha)\widehat{\overline{\beta f}}(-\alpha) = \underbrace{\beta\bar{\beta}}_{=1 \text{ since } \beta\in\mathsf{GF}(2^n)^*} \hat{f}(\alpha)\hat{\bar{f}}(-\alpha) = 1$ (because f is $\mathsf{GF}(2^n)$-bent).

Lemma 2. *Let* $f : G \to \mathsf{GF}(2^n)$. *Then the following equivalences hold*:

(1) $\forall x \in G^*,\ f(x) = 0$ *if and only if* $\forall \alpha \in G,\ \hat{f}(\alpha) = f(0)$;

(2) $\forall \alpha \in G^*,\ \hat{f}(\alpha) = 0$ *if and only if f is constant.*

Proof. (1) ($\Rightarrow$) $\hat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x) = f(0)\chi_\alpha(0) = f(0)$;

($\Leftarrow$) By the inversion formula: $f(x) = \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)} = f(0)\underbrace{\sum_{\alpha \in G} \chi_{-x}(\alpha)}_{=0 \text{ if } x \neq 0}$;

(2) ($\Rightarrow$) $f(x) = \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)} = \hat{f}(0)$;

($\Leftarrow$) $\hat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x) = \text{constant} \underbrace{\sum_{x \in G} \chi_\alpha(x)}_{=0 \text{ if } \alpha \neq 0}$.

Definition 10. Let $f : G \to \mathsf{GF}(2^n)^*$. Then we define its *derivative* in $\alpha \in G$ by

$$\begin{aligned} d_\alpha f &: G \to \mathsf{GF}(2^n)^* \\ x &\mapsto \frac{f(\alpha + x)}{f(x)} = f(\alpha + x)\overline{f(x)}. \end{aligned} \tag{53}$$

This derivative is exactly the one presented in Section 2 with a group H in a multiplicative representation.

Lemma 3. *Let* $f : G \to \mathsf{GF}(2^n)$. *Then we define the autocorrelation function of f,*

$$\begin{aligned} AC_f &: G \to \mathsf{GF}(2^n) \\ \alpha &\mapsto \sum_{x \in G} d_\alpha f(x). \end{aligned} \tag{54}$$

Then for all $\alpha \in G$,

$$\widehat{AC_f}(\alpha) = \hat{f}(\alpha)\hat{\bar{f}}(-\alpha). \tag{55}$$

Proof.

$$\begin{aligned}\widehat{AC_f}(\alpha) &= \sum_{x\in G} AC_f(x)\chi_\alpha(x)\\ &= \sum_{x\in G}\sum_{y\in G} d_x f(y)\chi_\alpha(x)\\ &= \sum_{x\in G}\sum_{y\in G} f(x+y)\overline{f(y)}\chi_\alpha(x+y)\overline{\chi_\alpha(y)}\\ &= \hat{f}(\alpha)\hat{\overline{f}}(-\alpha). \end{aligned} \tag{56}$$

Theorem 8. *A function* $f : G \to \mathsf{GF}(2^n)^*$ *is* $\mathsf{GF}(2^n)$*-bent if and only if for each* $\alpha \in G^*$ *its autocorrelation function is identically null, i.e.,* $\forall\alpha \in G^*$,

$$\sum_{x\in G} d_\alpha f(x) = 0. \tag{57}$$

Proof. Let $\alpha \in G^*$. Then

$\forall\alpha \in G^*,\ AC_f(\alpha) = 0$

$\Leftrightarrow \forall\alpha \in G,\ \widehat{AC_f}(\alpha) = AC_f(0)$ (according to Lemma 2)

$\Leftrightarrow \forall\alpha \in G,\ \hat{f}(\alpha)\hat{\overline{f}}(-\alpha) = \sum_{x\in G} f(x)\overline{f(x)}$ (according to Lemma 3)

$\Leftrightarrow \forall\alpha \in G,\ \hat{f}(\alpha)\hat{\overline{f}}(-\alpha) = |\,G\,|(\mathrm{mod}\ 2) = 1$ (because *f* is $\mathsf{GF}(2^n)^*$-valued).

(58)

This result seems very similar to Proposition 3.

7.2. Construction of a $\mathsf{GF}(2^n)$-bent function

Let *g* be any function from *G* to $\mathsf{GF}(2^n)$ and let define

$$\begin{aligned} f : G^2 &\to \mathsf{GF}(2^n)^* \\ (x,\ y) &\mapsto \chi_x(y)g(y). \end{aligned} \tag{59}$$

Then f is $\mathsf{GF}(2^n)$-bent.

Indeed we have

$$\begin{aligned} d_{(\alpha,\beta)}f(x,\ y) &= f(\alpha + x,\ \beta + y)\overline{f(x,\ y)} \\ &= \chi_{\alpha+x}(\beta + y)g(\beta + y)\overline{\chi_x(y)}\,\overline{g(y)} \\ &= \chi_\alpha(\beta + y)\chi_x(\beta + y)g(\beta + y)\overline{\chi_x(y)}\,\overline{g(y)} \\ &= \chi_\alpha(\beta)\chi_\alpha(y)\chi_x(\beta)\chi_x(y)g(\beta + y)\overline{\chi_x(y)}\,\overline{g(y)} \\ &= \chi_\alpha(\beta)\chi_\alpha(y)g(\beta + y)\overline{g(y)}\chi_\beta(x) \text{ (because } \chi_x(\beta) = \chi_\beta(x)). \end{aligned} \tag{60}$$

So for $(\alpha,\ \beta) \in G^2 \setminus \{(0,\ 0)\}$, we have

$$\begin{aligned} &\sum_{(x,\ y)\in G^2} d_{(\alpha,\beta)}f(x,\ y) \\ &= \sum_{(x,\ y)\in G^2} \chi_\alpha(\beta)\chi_\alpha(y)g(\beta + y)\overline{g(y)}\chi_\beta(x) \\ &= \chi_\alpha(\beta)\sum_{y\in G}\chi_\alpha(y)g(\beta + y)\overline{g(y)}\underbrace{\sum_{x\in G}\chi_\beta(x)}_{=0 \text{ if } \beta\neq 0} \\ &= \begin{cases} 0 & \text{if } \beta \neq 0, \\ \underbrace{|G|(\mathrm{mod}\ 2)}_{=1}\underbrace{\chi_\alpha(0)}_{=1}\sum_{y\in G}\chi_\alpha(y) \quad \underbrace{g(0 + y)\overline{g(y)}}_{=1 \text{ because } g(y)\in\mathsf{GF}(2^n)^*} & \text{if } \beta = 0 \text{ (and then } \alpha \neq 0). \end{cases} \end{aligned} \tag{61}$$

In particular we have

$$\sum_{(x,\,y)\in G^2} d_{(\alpha,\,0)}f(x,\ y) = \sum_{y\in G}\chi_\alpha(y)$$

$$= 0 \quad (\text{because } \alpha \neq 0). \tag{62}$$

We can also show that a particular instance of such functions is also additively perfect nonlinear. Let γ be a primitive root of $\mathsf{GF}(2^n)$ and $G = \mathsf{GF}(p)^m$. We have $\chi_x(y) = \gamma^{x\cdot y} = e_\gamma(x \cdot y)$. We already know that the function $f : (x,\ y) \mapsto \chi_x(y)$ is bent (it is sufficient to choose for g the map $y \in G \mapsto 1 \in \mathsf{GF}(2^n)^*$). In particular if $G = (\mathsf{GF}(p))^2$, then we have $\chi_x(y) = e_\gamma(xy)$. Let us see that f is perfect nonlinear. Let $(\alpha,\ \beta) \in (\mathsf{GF}(p))^2\setminus\{(0,\ 0)\}$ and $\varepsilon \in \mathsf{GF}(2^n)^*$. Then

$$\varepsilon = d_{(\alpha,\,\beta)}f(x,\ y)$$

$$\Leftrightarrow \varepsilon = e_\gamma((\alpha + x)(\beta + y))\overline{e_\gamma(xy)}$$

$$\Leftrightarrow \varepsilon = e_\gamma(\alpha\beta)e_\gamma(\alpha y)e_\gamma(\beta x)\underbrace{e_\gamma(xy)\overline{e_\gamma(xy)}}_{=1}$$

$$\Leftrightarrow \varepsilon = e_\gamma(\alpha\beta)e_\gamma(\alpha y)e_\gamma(\beta x). \tag{63}$$

1. Let us suppose that $\alpha = 0$ (and then $\beta \neq 0$). Then we have

$$d_{(0,\,\beta)}f(x,\ y) = \varepsilon$$

$$\Leftrightarrow e_\gamma(\beta x) = \varepsilon$$

$$\Leftrightarrow \beta x = l_\gamma(\varepsilon)$$

$$\Leftrightarrow x = \frac{1}{\beta}l_\gamma(\varepsilon) \quad (\beta \neq 0). \tag{64}$$

Therefore the solutions have the form $\left(\frac{1}{\beta} l_\gamma(\varepsilon),\ y\right)$ for each $y \in \mathsf{GF}(p)$. So there are exactly $|\mathsf{GF}(p)| = p$ such solutions.

2. Let us suppose that $\beta = 0$ (and then $\alpha \neq 0$). Then we have

$$\begin{aligned} & d_{(\alpha, 0)} f(x,\ y) = \varepsilon \\ \Leftrightarrow\ & e_\gamma(\alpha y) = \varepsilon \\ \Leftrightarrow\ & \alpha y = l_\gamma(\varepsilon) \\ \Leftrightarrow\ & y = \frac{1}{\alpha} l_\gamma(\varepsilon) \quad (\alpha \neq 0). \end{aligned} \tag{65}$$

Therefore the solutions have the form $\left(x,\ \frac{1}{\alpha} l_\gamma(\varepsilon)\right)$ for each $x \in \mathsf{GF}(p)$. So there are exactly $|\mathsf{GF}(p)| = p$ such solutions.

3. Let us suppose that $\alpha \neq 0$ and $\beta \neq 0$. Then we have

$$\begin{aligned} & d_{(0, \beta)} f(x,\ y) = \varepsilon \\ \Leftrightarrow\ & e_\gamma(\alpha\beta) e_\gamma(\alpha y) e_\gamma(\beta x) = \varepsilon \\ \Leftrightarrow\ & e_\gamma(\alpha y + \beta x) = \frac{1}{e_\gamma(\alpha\beta)} = \varepsilon \\ \Leftrightarrow\ & \alpha y + \beta x = l_\gamma\left(\frac{1}{e_\gamma(\alpha\beta)}\varepsilon\right) \\ \Leftrightarrow\ & \alpha y + \beta x = -\alpha\beta + l_\gamma(\varepsilon) \\ \Leftrightarrow\ & x = \frac{1}{\beta}(-\alpha y - \alpha\beta + l_\gamma(\varepsilon)). \end{aligned} \tag{66}$$

Therefore the solutions have the form $\left(\frac{1}{\beta}(-\alpha y - \alpha\beta + l_\gamma(\varepsilon)),\ y\right)$ for each $y \in \mathsf{GF}(p)$. So there are exactly $|\mathsf{GF}(p)| = p$ such solutions.

Therefore $|\{(x, y) \in \mathsf{GF}(p)^2 \,|\, d_{(\alpha,\beta)}f(x, y) = \varepsilon\}| = p = \frac{p^2}{p} = \frac{|(\mathsf{GF}(p))^2|}{|\mathsf{GF}(p)^*|}$.

Thus f is perfect nonlinear. A question raised by the new approach of bentness is to know whether or not this is equivalent - as in the traditional setting - to perfect nonlinearity. The answer is « no » as we can see in the following subsection.

7.3. Links between $\mathsf{GF}(2^n)$-bentness and perfect nonlinearity

Theorem 9. *Let* $f : G \to \mathsf{GF}(2^n)^*$. *If f is perfect nonlinear, then f is* $\mathsf{GF}(2^n)$*-bent. The reciprocal assertion is not valid.*

Proof. The group G is isomorphic to a certain direct product C_p^m. Since f is perfect nonlinear, for all $\alpha \in G^*$ and for all $\beta \in \mathsf{GF}(2^n)^*$, we have

$$|\{x \in G \,|\, d_\alpha f(x) = \beta\}| = \frac{(2^n - 1)^m}{2^n - 1} = (2^n - 1)^{m-1}. \tag{67}$$

So we have also

$$\begin{aligned}\sum_{x \in G} d_\alpha f(x) &= \sum_{y \in \mathsf{GF}(2^n)^*} |\{x \in G \,|\, d_\alpha f(x) = y\}|(\mathrm{mod}\ 2)y \\ &= \sum_{y \in \mathsf{GF}(2^n)^*} \underbrace{(2^n - 1)^{m-1}(\mathrm{mod}\ 2)}_{=1}y \\ &= \sum_{y \in \mathsf{GF}(2^n)^*} y \quad (\text{since } n \neq 1) \\ &= 0. \end{aligned} \tag{68}$$

Thus f is bent.

In order to prove that the reciprocal assertion is false, it is sufficient to find a $\mathsf{GF}(2^n)$-bent function which is not perfect nonlinear for a given configuration of G and $\mathsf{GF}(2^n)$. Let $p = 3 = 2^n - 1$. Let us suppose that $G = \mathsf{GF}(3)^2$. We consider that $\mathsf{GF}(4) = \{0, 1, \gamma, \gamma + 1\}$ with $\gamma^2 = \gamma + 1$ (with γ a primitive root). Let $(x_0, y_0) \in \mathsf{GF}(3)^2$ and $(\gamma_1, \gamma_2) \in (\mathsf{GF}(4)^*)^2$ such that $\gamma_1 \neq \gamma_2$. Finally we define the following function:

$$f : \mathsf{GF}(3)^2 \to \mathsf{GF}(4)^*$$

$$(x, y) \mapsto \gamma_1 1_{\mathsf{GF}(3)^2 \setminus \{(x_0, y_0)\}}(x, y) + \gamma_2 1_{\{(x_0, y_0)\}}(x, y), \qquad (69)$$

where 1_S denotes the indicator function of a set S (in particular $1_{\{(x_0, y_0)\}}$ is equal to $\delta_{(x_0, y_0)}$ the Dirac mass in (x_0, y_0) previously introduced). We now prove that $\forall(\alpha, \beta) \in \mathsf{GF}(3)^2 \setminus \{(0, 0)\}$, $\sum_{(x, y) \in \mathsf{GF}(3)^2} d_{(\alpha, \beta)} f(x, y) = 0$ (which by Theorem 8 implies that f is $\mathsf{GF}(2^n)$-bent) but f is not perfect nonlinear.

So let $(\alpha, \beta) \in \mathsf{GF}(3)^2 \setminus \{(0, 0)\}$. If

$$(x, y) \notin \{(x_0, y_0), (-\alpha + x_0, -\beta + y_0)\},$$

then

$$f(x, y) = f(\alpha + x, \beta + y) = \gamma_1$$

and thus $d_{(\alpha, \beta)} f(x, y) = \gamma_1 \overline{\gamma_1} = 1$. Now if $(x, y) = (x_0, y_0)$, then we have $f(x, y) = \gamma_2$ and $f(\alpha + x, \beta + y) = \gamma_1$ and so $d_{(\alpha, \beta)} f(x, y) = \gamma_1 \overline{\gamma_2}$. Finally if $(x, y) = (-\alpha + x_0, -\beta + y_0)$, then $f(x, y) = \gamma_1$ and $f(\alpha + x, \beta + y) = \gamma_2$ and so $d_{\alpha, \beta} f(x, y) = \gamma_2 \overline{\gamma_1}$. Let us show that $1 \neq \gamma_1 \overline{\gamma_2}$, $1 \neq \overline{\gamma_1} \gamma_2$ and $\gamma_1 \overline{\gamma_2} \neq \overline{\gamma_1} \gamma_2$. Since $\gamma_1 \neq \gamma_2$, $1 \neq \gamma_1 \overline{\gamma_2}$ and $1 \neq \overline{\gamma_1} \gamma_2$. Now let us suppose that $\gamma_1 \overline{\gamma_2} = \overline{\gamma_1} \gamma_2$. This is equivalent to $\gamma_1^2 = \gamma_2^2$. Since $\gamma_1 \neq \gamma_2$, this implies that $1 = \gamma^2$ or $\gamma^2 = \gamma$ which is obviously impossible in $\mathsf{GF}(4)^*$. So we can see that

$$|\{(x,\ y) \in \mathsf{GF}(3)^2 \,|\, d_{(\alpha,\beta)}f(x,\ y) = 1\}| = 7,$$

$$|\{(x,\ y) \in \mathsf{GF}(3)^2 \,|\, d_{(\alpha,\beta)}f(x,\ y) = \gamma_1\overline{\gamma_2}\}| = 1$$

and

$$|\{(x,\ y) \in \mathsf{GF}(3)^2 \,|\, d_{(\alpha,\beta)}f(x,\ y) = \overline{\gamma_1}\gamma_2\}| = 1.$$

So in particular *f* is not perfect nonlinear and

$$\sum_{(x,y)\in\mathsf{GF}(3)^2} d_{(\alpha,\beta)}f(x,\ y) = 7\,(\mathrm{mod}\ 2)1 + \gamma\overline{\gamma_2} + \overline{\gamma_1}\gamma_2 = 1 + \gamma + \gamma^2 = 0$$

so according to Theorem 8, *f* is $\mathsf{GF}(2^n)$-bent.

The concept of $\mathsf{GF}(2^n)$-bent function is then weaker than classical bentness. But one can also define a weaker notion of perfect nonlinearity.

7.4. Modulo 2 perfect nonlinearity

Definition 11. Let X and Y be two finite nonempty sets. Then a function $f : X \to Y$ is called *modulo* 2 *balanced* if for each $y \in Y$,

$$|\{x \in X\,|\, f(x) = y\}| = \frac{|X|}{|Y|}(\mathrm{mod}\ 2). \tag{70}$$

Note 2.

- The equality $\frac{|X|}{|Y|}(\mathrm{mod}\ 2) = 0$ holds if and only if $|X| = 2k|Y|$. In particular $|X|$ is an even integer;

- The equality $\frac{|X|}{|Y|}\pmod 2 = 1$ holds if and only if $|X| = (2k+1)|Y|$;

- If $|X|$ and $|Y|$ are odd and $|Y|$ divides $|X|$, then $\frac{|X|}{|Y|}\pmod 2 = 1$.

  In particular if $|X| = p^m$ and $|Y| = p^l$ with $m \geq l$, then $\frac{|X|}{|Y|}\pmod 2$ $= 1$.

Lemma 4. *Let H be an elementary finite Abelian p-group and X be a finite nonempty set such that $|H|$ divides $|X|$, $|X|$ and $|H|$ are odd. A function $f : X \to H$ is modulo 2 balanced if and only if for each $\beta \in H^*$, $\sum_{x\in X} \xi_\beta \circ f(x) = 0$ (where ξ_β denotes an element of the $\mathsf{GF}(2^n)$-dual group of H).*

Proof. Let $f : X \to H$ be any function. Then we have

$$\sum_{x\in X} \xi_\beta \circ f(x) = \sum_{y\in H} |\{x \in X \,|\, f(x) = y\}| \pmod 2 \xi_\beta(y)$$

$$= \widehat{\mu_f}(\beta), \tag{71}$$

where we define

$$\mu_f : H \to \mathsf{GF}(2) \subset \mathsf{GF}(2^n)$$

$$y \mapsto |\{x \in X \,|\, f(x) = y\}| \pmod 2. \tag{72}$$

Now let us suppose that f is modulo 2 balanced. Then $\forall \beta \in H$,

$$\sum_{x\in X} \xi_\beta \circ f(x) = \frac{|X|}{|H|}\pmod 2 \sum_{y\in H} \xi_\beta(y)$$

(according to formula (71)). By assumptions on X and H, $\frac{|X|}{|H|}\pmod 2$

$= 1$. Then

$$\sum_{x \in X} \xi_\beta \circ f(x) = \sum_{y \in H} \xi_\beta(y) = 0 \text{ for all } \beta \in H^*.$$

Let us suppose that for each $\beta \in H^*$,

$$\sum_{x \in X} \xi_\beta \circ f(x) = 0.$$

Then according to formula (71), for each $\beta \in H^*$, $\widehat{\mu_f}(\beta) = 0$. So by Lemma 2, μ_f is constant equal to $b \in \{0, 1\}$. Moreover $\{\{x \in X \mid f(x) = y\}\}_{y \in H}$ is a partition of X and then $|X| = \sum_{y \in Y} |\{x \in X \mid f(x) = y\}|$. If we suppose that μ_f is uniformly equal to 0, then it means that $|X|$, as a sum of even numbers, is an even integer which is a contradiction and thus $\mu_f = 1$. Then by definition of μ_f we deduce that f is modulo 2 balanced.

We can also prove a weaker result but in a more general framework.

Lemma 5. *Let H be an elementary finite Abelian p-group and X be a finite nonempty set such that $|H|$ divides $|X|$. If a map $f : X \to H$ is modulo* 2 *balanced, then* $\forall \beta \in H^*$, $\sum_{x \in X} \xi_\beta \circ f(x) = 0$.

Proof. Let $\beta \in H^*$. Then we have

$$\sum_{x \in X} \xi_\beta \circ f(x) = \sum_{y \in H} |\{x \in X \mid f(x) = y\}| (\mathrm{mod}\ 2) \xi_\beta(y)$$

$$= \frac{|X|}{|H|} (\mathrm{mod}\ 2) \sum_{x \in X} \xi_\beta(y)$$

(since f is modulo 2 balanced). If $\frac{|X|}{|H|} (\mathrm{mod}\ 2) = 0$, the result is obvious.

So let us suppose that $\frac{|X|}{|H|} \pmod 2 = 1$. Then we have

$$\sum_{x\in X} \xi_\beta \circ f(x) = \sum_{y\in H} \xi_\beta(y) = 0 \quad \text{(because } \beta \in H^*\text{)}.$$

Definition 12. Let G and H be any finite groups. Then a map $f : G \to H$ is called *modulo* 2 *perfect nonlinear* if for each $\alpha \in G^*$, the derivative of f in direction α is modulo 2 balanced.

It is obvious that a classical perfect nonlinear function is also modulo 2 perfect nonlinear. But we have built in the proof of Theorem 9, a function $f : \mathsf{GF}(3)^2 \to \mathsf{GF}(4)^*$ which is modulo 2 perfect nonlinear but not classical perfect nonlinear.

In particular configurations of groups G and H, we can develop a dual characterization of modulo 2 perfect nonlinearity using $\mathsf{GF}(2^n)$-bentness that generalizes Theorem 1.

Theorem 10. *Let G and H be two elementary finite Abelian p-groups such that* $|H|$ *divides* $|G|$. *Then a map* $f : G \to H$ *is modulo* 2 *perfect nonlinear if and only if for each* $\beta \in H^*$, *the map* $\xi_\beta \circ f : G \to \mathsf{GF}(2^n)^*$ *is* $\mathsf{GF}(2^n)$*-bent.*

Proof. Since $|G| = p^m$ and $|H| = p^l$ and $\frac{|G|}{|H|} = p^{m-l}$, we can apply Lemma 4: f is modulo 2 perfect nonlinear if and only if $\forall \alpha \in G^*$, $d_\alpha f$ is modulo 2 balanced if and only if $\forall \alpha \in G^*$ and $\forall \beta \in H^*$,

$$\sum_{x\in X} \xi_\beta \circ d_\alpha f(x) = 0.$$

But $\xi_\beta \circ d_\alpha f(x) = \xi_\beta(f(\alpha + x) - f(x)) = \xi_\beta(f(\alpha + x))\overline{\xi_\beta(f(x))} = d_\alpha \xi_\beta \circ f(x)$.

Then f is modulo 2 perfect nonlinear if and only if $\forall\beta \in H^*$, $\forall\alpha \in G^*$,

$$\sum_{x\in X} d_\alpha \xi_\beta \circ f(x) = 0$$

which, according to Theorem 8, is equivalent to the fact that for each $\beta \in H^*$, $\xi_\beta \circ f$ is $\mathsf{GF}(2^n)$-bent.

Finally let us see the case of $\mathsf{GF}(2^n)^*$-valued functions. So we need to consider the $\mathsf{GF}(2^n)$-dual group of $\mathsf{GF}(2^n)^*$ itself.

Lemma 6. *Let* γ *be a primitive root of* $\mathsf{GF}(2^n)$. *Then the* $\mathsf{GF}(2^n)$-*character associated to* γ^i *is*

$$\begin{aligned}\xi_{\gamma^i} : \mathsf{GF}(2^n)^* &\to \mathsf{GF}(2^n)^* \\ \gamma^j &\mapsto \gamma^{ij}.\end{aligned} \tag{73}$$

In particular ξ_γ *is the identity function of* $\mathsf{GF}(2^n)^*$.

More precisely we have $\widehat{\mathsf{GF}(2^n)^*} = \langle \xi_\gamma \rangle = \{\xi_\gamma^i \mid i \in \mathsf{GF}(p)\}$ *and* $\xi_{\gamma^i} = \xi_\gamma^i$.

Proof. The form of the $\mathsf{GF}(2^n)$-characters of $\mathsf{GF}(2^n)^*$ is a particular instance of the characters given in Note 1. The fact that ξ_γ is the identity function of $\mathsf{GF}(2^n)^*$ is obvious. We only need to check that the order of ξ_γ is equal to $p = 2^n - 1$. Since $\xi_\gamma^p(\gamma^i) = (\gamma^i)^p = 1$ for each $\gamma^i \in \mathsf{GF}(2^n)^*$, the order of ξ is at most p. But $\xi_\gamma^{p-1}(\gamma) = \gamma^{p-1} \neq 1$, so the order of ξ is exactly p and therefore $\widehat{\mathsf{GF}(2^n)^*}$ is generated by ξ_γ. Finally $\xi_{\gamma^i}(\gamma^j) = \gamma^{ij} = (\gamma^j)^i$ $= \chi_\gamma^i(\gamma^j)$.

Proposition 6. *Let G be an elementary finite Abelian p-group. Let*

$f : G \to \mathsf{GF}(2^n)^*$. *Then f is modulo* 2 *perfect nonlinear* $\Leftrightarrow \forall i \in \mathsf{GF}(p)^*$, *the map*

$$f^i : G \to \mathsf{GF}(2^n)^*$$

$$x \mapsto (f(x))^i \tag{74}$$

is $\mathsf{GF}(2^n)$*-bent. In particular f is* $\mathsf{GF}(2^n)$*-bent.*

Proof. According to Theorem 10, f is modulo 2 perfect nonlinear if and only if for each $\beta \in \mathsf{GF}(2^n)^* \setminus \{1\}$, $\xi_\beta \circ f$ is $\mathsf{GF}(2^n)$-bent. This is equivalent to the fact that for each $i \in \mathsf{GF}(p)^*$, $\xi_{\gamma^i} \circ f$ is $\mathsf{GF}(2^n)$-bent (with γ a primitive root of $\mathsf{GF}(2^n)$). According to Lemma 6, for each $x \in G$, $\xi_{\gamma^i}(f(x)) = (f(x))^i$. Therefore $\forall i \in \mathsf{GF}(p)^*$, f^i is $\mathsf{GF}(2^n)$-bent.

7.5. Generalization with group actions

In this section, we translate the generalized notion of perfect nonlinearity (see 2) in our characteristic 2 setting and we give its characterization in terms of the modulo 2 Fourier transform that generalizes both Theorems 2 and 10.

Definition 13. Let G be a finite group that acts faithfully on a finite nonempty set X and H be any finite group. Then a function $f : X \to H$ is called *modulo* 2 *perfect nonlinear* (*with respect to the action of G on X*) if for each $\alpha \in G^*$, the derivative $d_\alpha f : x \in X \mapsto f(\alpha \cdot x) - f(x) \in H$ is modulo 2 balanced.

If $G = X$ and we consider the regular action by translation, then the previous notion becomes modulo 2 perfect nonlinearity.

Let G be an elementary finite Abelian p-group that acts on a finite nonempty set X. Let $(\phi, \psi) \in (\mathsf{GF}(2^n)^G)^2$. Then we define a *skew* convolutional product

$$\phi \boxtimes \psi : G \to \mathsf{GF}(2^n)$$

$$\alpha \mapsto (\phi \boxtimes \psi)(\alpha) := \sum_{x \in X} \phi(x)\psi(\alpha \cdot x). \tag{75}$$

Lemma 7. *With the previous assumptions on* G, X, ϕ *and* ψ, *we have for all* $\alpha \in G$,

$$\widehat{(\phi \boxtimes \psi)}(\alpha) := \sum_{x \in X} \widehat{\phi_x}(-\alpha)\widehat{\psi_x}(\alpha), \tag{76}$$

where for each $x \in X$ *and any map* $\theta : G \to Y$ (*Y being any set*), *we define*

$$\theta_x : G \to Y$$

$$\alpha \mapsto \theta(\alpha \cdot x). \tag{77}$$

Proof.

$$\widehat{(\phi \boxtimes \psi)}(\alpha) = \sum_{g \in G} \sum_{x \in X} \phi(x)\psi(g \cdot x)\chi_\alpha(g)$$

$$= \sum_{x \in X} \phi(x) \sum_{g \in G} \psi(g \cdot x)\chi_\alpha(g). \tag{78}$$

But $\forall h \in G$,

$$\sum_{g \in G} \psi(g \cdot x)\chi_\alpha(g) = \sum_{g \in G} \psi((g-h) \cdot x)\chi_\alpha(g-h)$$

$$= \sum_{g \in G} \psi((g-h) \cdot x)\chi_\alpha(g)\overline{\chi_\alpha(h)}.$$

Therefore $\forall h \in G$,

$$\widehat{(\phi \boxtimes \psi)}(\alpha) = \sum_{x \in X} \phi(x)\overline{\chi_\alpha(h)} \sum_{g \in G} \psi((g-h) \cdot x)\chi_\alpha(g)$$

$$= \sum_{x\in X}\phi(x)\overline{\chi_\alpha(h)}\sum_{g\in G}\psi((g\cdot(-h\cdot x)))\chi_\alpha(g)$$

$$= \sum_{y\in X}\phi(h\cdot y)\overline{\chi_\alpha(h)}\sum_{g\in G}\psi(g\cdot y)\chi_\alpha(g)$$

(change of variable $y := -h \cdot x$)

$$= \sum_{y\in X}\phi(h\cdot y)\overline{\chi_\alpha(h)}\widehat{\psi_y}(\alpha). \tag{79}$$

So when we sum over all $h \in G$,

$$\sum_{h\in G}(\phi\boxtimes\psi)(\alpha) = (\phi\boxtimes\psi)(\alpha)\underbrace{\sum_{h\in G}1}_{=|G|(\text{mod }2)=1} = \sum_{x\in X}\widehat{\psi_x}(\alpha)\sum_{h\in G}\phi(h\cdot x)\overline{\chi_\alpha(h)}$$

$$= \sum_{x\in X}\widehat{\phi_x}(-\alpha)\widehat{\psi_x}(\alpha). \tag{80}$$

The result above generalizes the trivialization of the convolutional product for the classical (see equality (13)) and the modulo 2 (see Proposition 4) Fourier transforms.

Lemma 8. *Let us suppose that G and H are two elementary finite Abelian p-groups such that G acts faithfully on a nonempty finite set X. Let $f : X \to H$. For $\beta \in H$, we define the autocorrelation function of f by*

$$AC_{f,\beta} : G \to \mathsf{GF}(2^n)$$

$$\alpha \mapsto \sum_{x\in X}\xi_\beta \circ d_\alpha f(x). \tag{81}$$

Then $\forall\alpha \in G$,

$$\widehat{AC_{f,\beta}}(\alpha) = \sum_{x\in X}\overline{\widehat{(\xi_\beta\circ f_x)}}(-\alpha)\widehat{(\xi_\beta\circ f_x)}(\alpha). \tag{82}$$

Proof.

$$\begin{aligned}\widehat{AC_{f,\beta}}(\alpha) &= \sum_{g\in G} AC_{f,\beta}(g)\chi_\alpha(g)\\ &= \sum_{g\in G}\sum_{x\in X}\xi_\beta\circ d_g f(x)\chi_\alpha(g)\\ &= \sum_{g\in G}\sum_{x\in X}\xi_\beta(f(g\cdot x))\overline{\xi_\beta(f(x))}\chi_\alpha(g)\\ &= \sum_{g\in G}(\overline{\xi_\beta\circ f}\boxtimes\xi_\beta\circ f)(g)\chi_\alpha(g)\\ &= (\widehat{\overline{\xi_\beta\circ f}\ \boxtimes\xi_\beta\circ f})(\alpha)\\ &= \sum_{x\in X}\widehat{\overline{(\xi_\beta\circ f)_x}}(-\alpha)(\widehat{\xi_\beta\circ f})_x(\alpha)\ \text{(according to Lemma 7)}\\ &= \sum_{x\in X}\widehat{\overline{(\xi_\beta\circ f_x)}}(-\alpha)(\widehat{\xi_\beta\circ f_x})(\alpha). \qquad (83)\end{aligned}$$

Theorem 11. *Let us suppose that G and H are two elementary finite Abelian p-groups such that G acts faithfully on a nonempty finite set X of odd cardinality and $|H|$ divides $|X|$. Then a function $f : X \to H$ is modulo* 2 *perfect nonlinear* (*with respect to the action of G on X*) *if and only if* $\beta \in H^*$, $\forall\alpha\in G$,

$$\sum_{x\in X}\widehat{\overline{(\xi_\beta\circ f_x)}}(-\alpha)(\widehat{\xi_\beta\circ f_x})(\alpha) = 1. \qquad (84)$$

Proof.

f is modulo 2 perfect nonlinear (with respect to the action of G on X)

$\Leftrightarrow\ \forall\alpha\in G^*,\ d_\alpha f$ is modulo 2 balanced

$$\Leftrightarrow \forall \alpha \in G^*, \forall \beta \in H^*, \sum_{x \in X} \xi_\beta \circ d_\alpha f(x) = 0 \text{ (according to Lemma 4)}$$

$$\Leftrightarrow \forall \alpha \in G^*, \forall \beta \in H^*, AC_{f,\beta}(\alpha) = 0$$

$$\Leftrightarrow \forall \alpha \in G, \forall \beta \in H^*, \widehat{AC_{f,\beta}}(\alpha) = AC_{f,\beta}(0) \text{ (by Lemma 2)}$$

$$\Leftrightarrow \forall \alpha \in G, \forall \beta \in H^*, \sum_{x \in X} \overline{(\widehat{\xi_\beta \circ f_x})}(-\alpha)(\widehat{\xi_\beta \circ f_x})(\alpha) = \sum_{x \in X} \xi_\beta(d_0 f(x))$$

(according to Lemma 8)

$$\Leftrightarrow \forall \alpha \in G, \forall \beta \in H^*, \sum_{x \in X} \overline{(\widehat{\xi_\beta \circ f_x})}(-\alpha)(\widehat{\xi_\beta \circ f_x})(\alpha)$$

$$= \sum_{x \in X} \xi_\beta(0) = |X| \ (\mathrm{mod}\ 2) = 1. \quad (85)$$

This result generalizes the equivalences of classical (Theorem 1) and group actions (Theorem 2) versions of perfect nonlinearity using the Fourier transform.

7.6. Modulo 2 relative difference sets

Definition 14. Let G be any finite group that acts faithfully on a finite nonempty set X of cardinality v. Let H be a finite group of cardinality m. We define the faithful action of $G \times H$ on $X \times H$ by $(g, h) \cdot (x, h') := (g \cdot x, h + h')$ for $(x, g, h, h') \in X \times G \times H \times H$, i.e., it is the action of G on X on the first component and the regular action of H on the second component. Let $R \subset X \times H$ of cardinality k. Then R is called a *modulo* 2 $G \times H$-(v, m, k, λ)*-difference set of* $X \times H$ *relative to* $\{0\} \times H$ if

1. for every $(g, h) \neq (0, h) \in G \times H$,

$$|\{((x_1, h_1), (x_2, h_2)) \in R^2 \,|\, (g, h) \cdot (x_1, h_1) = (x_2, h_2)\}| \quad (86)$$

is a constant modulo 2. The constant is denoted as $\lambda \in$ GF(2);

2. if (x, h) and (x, h') belong to R, then $h = h'$.

Such a $G \times H$-(v, m, k, λ)-relative difference set is called *semiregular* if $v = k$.

Note that only axiom (1) has changed with respect to the definition of $G \times H$-relative difference sets introduced in the first part of this paper. In particular each $G \times H$-semiregular modulo 2 relative difference set R gives rise to a function $f : X \to H$ such that $R = \{(x, f(x)) | x \in X\}$.

Theorem 12. *Let us suppose that G and H are two elementary finite Abelian p-groups such that G acts faithfully on a nonempty finite set X of odd cardinality and* $|H|$ *divides* $|X|$. *Then a function* $f : X \to H$ *is modulo* 2 *perfect nonlinear* (*with respect to the action of G on X*) *if and only if the set* $R := \{(x, f(x)) | x \in X\}$ *is a semiregular modulo* 2 $G \times H$-$(v, m, k, 1)$-*difference set of* $X \times H$ *relative to* $\{0\} \times H$.

Proof. Since f is a mapping, $|R| = |G|$ and therefore we need to prove that f is G-perfect nonlinear if and only if R satisfies axiom (1) of modulo 2 $G \times H$-relative difference sets with $\lambda = \frac{|X|}{|H|} \pmod 2 = \frac{v}{m} \pmod 2 = 1$. This last assertion is equivalent to the following ones for each $(g, h) \in G^* \times H$,

$$|\{((x_1, h_1), (x_2, h_2)) \in R^2 | (g, h) \cdot (x_1, h_1) = (x_2, h_2)\}| \pmod 2 = 1$$

$$= \frac{|X|}{|H|} \pmod 2$$

$$\Leftrightarrow |\{((x_1, h_1), (x_2, h_2)) \in R^2 | (g \cdot x_1, h + f(x_1)) = (x_2, f(x_2))\}| \pmod 2 = 1$$

$$= \frac{|X|}{|H|} \pmod 2$$

$$\Leftrightarrow |\{x \in X \mid f(g \cdot x) - f(x) = h\}| = \frac{|X|}{|H|} \pmod 2$$

$\Leftrightarrow$ f is modulo 2 perfect nonlinear

(with respect to the action of G on X).

In the proof of Theorem 9 is built a function $f : \mathrm{GF}(3)^2 \to \mathrm{GF}(4)^*$ which is modulo 2 perfect nonlinear but not classical perfect nonlinear. Then the set $R := \{((x, y), f(x, y)) \mid (x, y) \in \mathrm{GF}(3)^2\}$ is a semiregular modulo 2 $\mathrm{GF}(3)^2 \times \mathrm{GF}(4)^*$-$(9, 3, 9, 1)$ difference set of $\mathrm{GF}(3)^2 \times \mathrm{GF}(4)^*$ relative to $\{(0, 0)\} \times \mathrm{GF}(4)$ inequivalent to any classical semiregular relative difference sets with parameters $(9, 3, 9, 3)$.

References

[1] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptology 4(1) (1991), 3-72.

[2] C. Carlet and C. Ding, Highly nonlinear mappings, J. Complexity 20(2) (2004), 205-244.

[3] J. F. Dillon, Elementary Hadamard difference sets, Ph.D. Thesis, University of Maryland, 1974.

[4] FIPS 46-3, Data encryption standard, Federal Information Processing Standards Publication 46-3, U. S. Department of Commerce/N.I.S.T., 1999.

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

[6] M. Matsui, Linear cryptanalysis method for DES cipher, Advances in Cryptology - Eurocrypt' 93, Lecture Notes in Computer Science, Vol. 765, pp. 386-397, 1994.

[7] K. Nyberg, Perfect nonlinear *S*-boxes, Advances in Cryptology - Eurocrypt' 92, Lecture Notes in Computer Science, Vol. 547, pp. 378-386, 1992.

[8] L. Poinsot, Non linéarité parfaite généralisée au sens des actions de groupe, contribution aux fondements de la solidité cryptographique, Ph.D. Thesis, University of South Toulon-Var, 2005.

[9] L. Poinsot, Bent functions on a finite nonabelian group, J. Discrete Math. Sci. Crypt. 9(2) (2006), 349-364.

[10] L. Poinsot and S. Harari, Generalized Boolean bent functions, Progress in

Cryptology - Indocrypt 2004, Lecture Notes in Computer Science, Vol. 3348, pp. 107-119, 2004.

[11] L. Poinsot and S. Harari, Group actions based perfect nonlinearity, GESTS Internat. Trans. Comput. Sci. Eng. 12(1) (2005), 1-14.

[12] A. Pott, Nonlinear functions in abelian groups and relative difference sets, Discrete Appl. Math. 138 (2004), 177-193.

[13] O. S. Rothaus, On bent functions, J. Comb. Theo. A 20 (1976), 300-305.

[14] C. E. Shannon, Communication theory of secrecy systems, Bell Sys. Tech. J. 28 (1949), 656-715.

■