Harmonic analysis and a bentness-like notion in certain finite Abelian groups over some finite fields

Laurent Poinsot

Harmonic analysis and a bentness-like notion in certain finite Abelian groups over some finite fields

Laurent Poinsot

Université Paris 13, Paris Sorbonne Cité, LIPN, CNRS (UMR 7030), France

Abstract

It is well-known that degree two finite field extensions can be equipped with a Hermitian-like structure similar to the extension of the complex field over the reals. In this contribution, using this structure, we develop a modular character theory and the appropriate Fourier transform for some particular kind of finite Abelian groups. Moreover we introduce the notion of bent functions for finite field valued functions rather than usual complex-valued functions, and we study several of their properties. In particular we prove that this bentness notion is a consequence of that of Logachev, Salnikov and Yashchenko, introduced in *Bent functions on a finite Abelian group* (1997). In addition this new bentness notion is also generalized to a vectorial setting.

Keywords: Finite Abelian groups, character theory, Hermitian spaces, Fourier transform, bent functions.

2010 Mathematics Subject Classification Primary 11T24; Secondary 06E75; 11T71

1. Introduction

The most simple Hermitian structure is given by the complex field $\mathbb{C}$ when equipped with the complex modulus $\overline{z}$ (for $z \in \mathbb{C}$). Although quite simple, this structure has many applications in the theory of harmonic analysis of finite Abelian groups. Indeed the theory of characters for such groups is explicitly based on the existence of a special subgroup of the multiplicative group $\mathbb{C}^*$, the *unit sphere* or *group of roots of unity* $\mathcal{S}(\mathbb{C}) = \{ z \in \mathbb{C} \colon \overline{z}z = 1 \}$. This multiplicative group contains an isomorphic copy of each possible cyclic group. Thus it is possible to represent an abstract group G as a group $\widehat{G}$ of $\mathcal{S}(\mathbb{C})$-valued functions that preserves the group structure of G, called *characters*, which is isomorphic to G itself. These characters are the group homomorphisms from G to $\mathcal{S}(\mathbb{C})$. Moreover the dual group $\widehat{G}$ is also an orthogonal basis for the $|G|$-th dimensional vector space of $\mathbb{C}$-valued functions defined on G. This property makes it possible to carry out a harmonic analysis on finite Abelian groups using the (discrete) Fourier transform which is defined as the decomposition of a vector of $\mathbb{C}^G$ in the basis of characters.

Given a degree two extension $\mathrm{GF}(p^{2n})$ of $\mathrm{GF}(p^n)$, the Galois field with p^n elements where p is a prime number, we can also define a "conjugate" and thus a

Email address: laurent.poinsot@lipn.univ-paris13.fr (Laurent Poinsot)

Hermitian structure on $\mathrm{GF}(p^{2n})$ in a way similar to the relation $\mathbb{C}/\mathbb{R}$. In particular this makes possible the definition of a unit circle $\mathcal{S}(\mathrm{GF}(p^{2n}))$ which is a cyclic group of order p^n+1, subgroup of the multiplicative group $\mathrm{GF}(p^{2n})^*$ of invertible elements. The analogy with $\mathbb{C}/\mathbb{R}$ is extended in this paper by the definition of $\mathrm{GF}(p^{2n})$-valued characters of finite Abelian groups G as group homomorphisms from G to $\mathcal{S}(\mathrm{GF}(p^{2n}))$. But $\mathcal{S}(\mathrm{GF}(p^{2n}))$ does obviously not contain a copy of each cyclic group. Nevertheless if d divides p^n+1, then the cyclic group $\mathbb{Z}_d$ of modulo d integers embeds as a subgroup of this particular unit circle. It forces our modular theory of characters to be applied only to direct products of the form $G=\prod_{i=1}^{N}\mathbb{Z}_{d_i}^{m_i}$ where each d_i divides p^n+1. In addition we prove that these modular characters form an orthogonal basis (by respect to the Hermitian-like structure $\mathrm{GF}(p^{2n})$ over $\mathrm{GF}(p^n)$). This decisive property makes it possible the definition of an appropriate notion of Fourier transform for $\mathrm{GF}(p^{2n})$-valued functions, rather than $\mathbb{C}$-valued ones, defined on G, as their decompositions in the dual basis of characters. In this contribution we largely investigate several properties of this modular version of the Fourier transform similar to classical ones.

Traditionally an important cryptographic criterion can be naturally defined in terms of Fourier transform. Indeed *bent functions* are those functions $f:G\to\mathcal{S}(\mathbb{C})$ such that the magnitude of their Fourier transform $|\widehat{f}(\alpha)|^2$ is constant, equals to $|G|$. Such functions achieve the optimal possible resistance against the famous linear cryptanalysis of secret-key cryptosystems. Now using our theory of characters we can translate the bentness concept in our modular setting in order to treat the case of $\mathcal{S}(\mathrm{GF}(p^{2n}))$-valued functions defined on a finite Abelian group G. In this paper are also studied some properties of such functions. As a last contribution, we develop a vectorial notion of bent functions that concerns maps from G to $\mathrm{GF}(p^{2n})^l$ that explicitly uses an Hermitian structure of $\mathrm{GF}(p^{2n})^l$.

We warm the reader that the new notion of bentness presented hereafter is introduced as an illustration of this new finite-field valued character theory and its associated Fourier transform. The possible connections between usual bent functions (in particular those with values in a finite-field, see [1]) and our own definition are not all made clear in the present contribution. This paper should only be seen as a complete presentation of a general framework about modular harmonic analysis, given by a modular character theory and an associated modular Fourier transform, that should possibly be used for future research to make interesting connections with cryptographic Boolean functions. In this contribution we limit ourselves to point out that the objects introduced hereafter share many properties with their well-known counterparts. Deeper relationships, if they exist, are outside the scope of our current work. Nevertheless we mention the important assertion proved in this contribution: many usual bent functions in the sense of Logachev, Salnikov and Yashchenko (see [12]) are also bent functions in our finite-field setting.

2. Character theory: the classical approach

In this paper G always denotes a finite Abelian group (in additive representation), 0_G is its identity element. Moreover for all groups H, H^* is the set obtained from H by removing its identity element (therefore, $G^*=G\setminus\{0_G\}$). This last notation is in accordance with the usual notation $\mathbb{N}^*=\mathbb{N}\setminus\{0\}$.

The character theory of finite Abelian groups was originally introduced in order to embed algebraic structures into the complex field $\mathbb{C}$, and therefore to obtain geometric realizations of abstract groups as sets of complex transformations. The main relevant objects are the *characters*, *i.e.* the group homomorphisms from a finite Abelian group G to the unit circle $\mathcal{S}(\mathbb{C})$ of the complex field. The set of all such characters of G together with point-wise multiplication is denoted by $\widehat{G}$ and called the *dual group of* G. A classical result claims that G and its dual are isomorphic This property essentially holds because $\mathcal{S}(\mathbb{C})$ contains an isomorphic copy of all cyclic groups. Usually the image in $\widehat{G}$ of $\alpha \in G$ by such an isomorphism is denoted by χ_α. The complex vector space $\mathbb{C}^G$ of complex-valued functions defined on G can be equipped with an inner product defined for $f, g \in \mathbb{C}^G$ by

$$\langle f, g \rangle = \sum_{x \in G} f(x)\overline{g(x)} \tag{1}$$

where $\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$. With respect to this Hermitian structure, $\widehat{G}$ is an orthogonal basis, *i.e.*

$$\langle \chi_\alpha, \chi_\beta \rangle = \begin{cases} 0 & \text{if } \alpha \neq \beta, \\ |G| & \text{if } \alpha = \beta \end{cases} \tag{2}$$

for $\alpha, \beta \in G^2$. We observe that in particular (replacing β by 0_G),

$$\sum_{x \in G} \chi_\alpha(x) = \begin{cases} 0 & \text{if } \alpha \neq 0_G, \\ |G| & \text{if } \alpha = 0_G. \end{cases} \tag{3}$$

According to the orthogonality property, the notion of characters leads to some harmonic analysis of finite Abelian groups *via* a (discrete) Fourier transform.

Definition 2.1. Let G be a finite Abelian group and $f : G \to \mathbb{C}$. The (discrete) Fourier transform of f is defined as

$$\begin{array}{rccc} \widehat{f}\colon & G & \to & \mathbb{C} \\ & \alpha & \mapsto & \displaystyle\sum_{x \in G} f(x)\chi_\alpha(x) \ . \end{array} \tag{4}$$

The Fourier transform of a function f is essentially its decomposition in the basis $\widehat{G}$. This transform is invertible and one has an *inversion formula* for f,

$$f(x) = \frac{1}{|G|} \sum_{\alpha \in G} \widehat{f}(\alpha)\overline{\chi_\alpha(x)} \tag{5}$$

for each $x \in G$. More precisely the Fourier transform is an algebra isomorphism from $(\mathbb{C}^G, *)$ to $(\mathbb{C}^G, .)$ where the symbol "." denotes the point-wise multiplication of functions, while $*$ is the convolutional product defined for $f, g \in (\mathbb{C}^G)$ by

$$\begin{array}{rccc} f * g\colon & G & \to & \mathbb{C} \\ & \alpha & \mapsto & \displaystyle\sum_{x \in G} f(x)g(-x + \alpha) \end{array} \tag{6}$$

Since the Fourier transform is an isomorphism between the two algebras, the *trivialization of the convolutional product* holds for each $(f, g) \in (\mathbb{C}^G)^2$ and each $\alpha \in G$,

$$\widehat{(f * g)}(\alpha) = \widehat{f}(\alpha)\widehat{g}(\alpha) \ . \tag{7}$$

From these two main properties one can establish the following classical results.

Proposition 1. *Let G be a finite Abelian group and $f, g \in \mathbb{C}^G$. We have*

$$\sum_{x\in G} f(x)\overline{g(x)} = \frac{1}{|G|}\sum_{\alpha\in G} \widehat{f}(\alpha)\overline{\widehat{g}(\alpha)} \text{ (Plancherel formula),} \tag{8}$$

$$\sum_{x\in G} |f(x)|^2 = \frac{1}{|G|}\sum_{\alpha\in G} |\widehat{f}(\alpha)|^2 \text{ (Parseval equation)} \tag{9}$$

where $|z|$ is the complex modulus of $z \in \mathbb{C}$.

This paper is mostly dedicated to the study of a character theory for some finite Abelian groups over some finite fields rather than $\mathbb{C}$. In particular we provide similar results as those from this section. Obviously we need an Hermitian structure over the chosen finite field. This is the content of the next section.

3. Hermitian structure over finite fields

In this section we recall some results about an Hermitian structure in some kinds of finite fields. By analogy with the classical theory of characters (recalled in section 2), this particular structure is involved in the definition of a suitable theory of finite field-valued characters of some finite Abelian groups which is developed in section 4. This section is directly inspired from [9] of which we follow the notations, and generalized to any characteristic p.

Let p be a given prime number and q an even power of p, *i.e.*, there is $n \in \mathbb{N}^*$ such that $q = p^{2n}$, and in particular q is a square.

Assumption 1. From now on the parameters p, n, q are fixed as introduced above.

As usually $\mathrm{GF}(q)$ is the finite field of characteristic p with q elements and by construction $\mathrm{GF}(\sqrt{q})$ is a subfield of $\mathrm{GF}(q)$. The field $\mathrm{GF}(q)$, as an extension of degree 2 of $\mathrm{GF}(\sqrt{q})$, is also a vector space of dimension 2 over $\mathrm{GF}(\sqrt{q})$. This situation is similar to the one of $\mathbb{C}$ and $\mathbb{R}$. As $\mathrm{GF}(q)$ plays the role of $\mathbb{C}$, the Hermitian structure should be provided for it. Again according to the analogy $\mathbb{C}/\mathbb{R}$, we then need to determine a corresponding conjugate. In order to do this we use the *Frobenius automorphism* Frob of $\mathrm{GF}(q)$ defined by

$$\begin{array}{rccc} \mathrm{Frob}: & \mathrm{GF}(q) & \to & \mathrm{GF}(q) \\ & x & \mapsto & x^p \end{array} \tag{10}$$

and one of its powers

$$\begin{array}{rccc} \mathrm{Frob}_k: & \mathrm{GF}(q) & \to & \mathrm{GF}(q) \\ & x & \mapsto & x^{p^k}. \end{array} \tag{11}$$

In particular $\mathrm{Frob}_1 = \mathrm{Frob}$.

Definition 3.1. The *conjugate of* $x \in \mathrm{GF}(q)$ *over* $\mathrm{GF}(\sqrt{q})$ is denoted by $\overline{x}$ and defined as

$$\overline{x} = \mathrm{Frob}_n(x) = x^{p^n} = x^{\sqrt{q}}. \tag{12}$$

In particular, for every $n \in \mathbb{Z}$, $\overline{n1} = n1$. The field extension $\mathrm{GF}(q)/\mathrm{GF}(\sqrt{q})$ has amazing similarities with the extension $\mathbb{C}$ over the real numbers in particular regarding the conjugate.

Proposition 2. *Let $x_1, x_2 \in \mathrm{GF}(q)^2$, then*

1. $\overline{x_1 + x_2} = \overline{x_1} + \overline{x_2}$,
2. $\overline{-x_1} = -\overline{x_1}$,
3. $\overline{x_1 x_2} = \overline{x_1}\ \overline{x_2}$,
4. $\overline{\overline{x_1}} = x_1$.

Proof. The three first points come from the fact that Frob_n is a field homomorphism of $\mathrm{GF}(q)$. The last point holds since for each $x \in \mathrm{GF}(q)$, $x^q = x$. □

The *relative norm with respect to* $\mathrm{GF}(q)/\mathrm{GF}(\sqrt{q})$ is defined as

$$\mathrm{norm}(x) = x\overline{x} \tag{13}$$

for $x \in \mathrm{GF}(q)$, and it maps $\mathrm{GF}(q)$ to $\mathrm{GF}(\sqrt{q})$. We observe that $\mathrm{norm}(x) \in \mathrm{GF}(\sqrt{q})$ because $\sqrt{q}+1$ divides $q-1$, and $\mathrm{norm}(x) = 0$ if, and only if, $x = 0$.

The *unit circle* of $\mathrm{GF}(q)$ is defined as the set

$$\mathcal{S}(\mathrm{GF}(q)) = \{\, x \in \mathrm{GF}(q) \colon x\overline{x} = 1 \,\} \tag{14}$$

of all elements having relative norm 1. By construction $\mathcal{S}(\mathrm{GF}(q))$ is the group of $(\sqrt{q}+1)$-th roots of unity, and therefore it is a (multiplicative) cyclic group of order $\sqrt{q}+1$ since $\mathrm{GF}(q)^*$ is cyclic and $\sqrt{q}+1$ divides $q-1$. In what follows, $\mathcal{S}(\mathrm{GF}(q))$ will play exactly the same role as $\mathcal{S}(\mathbb{C})$ in the classical theory of characters.

Now let $\mathrm{GF}(q)^l$ be the l-dimensional vector space over $\mathrm{GF}(q)$, then the *Hermitian dot product* of two vectors $x = (x_1, \ldots, x_l)$ and $y = (y_1, \ldots, y_l)$ of $\mathrm{GF}(q)^l$ is

$$\langle x, y \rangle = \sum_{i=1}^{l} x_i \overline{y_i}\ . \tag{15}$$

Again, this kind of Hermitian dot product has properties similar to the natural Hermitian inner product on complex vector spaces. Let $\alpha, \beta \in \mathrm{GF}(q)$ and $x, y, z \in \mathrm{GF}(q)^l$, then

1. $\langle (\alpha x + \beta y), z \rangle = \alpha\langle x, z\rangle + \beta\langle y, z\rangle$ (*linearity*),
2. $\langle x, y\rangle = \overline{\langle y, x\rangle}$ (conjugate symmetry),
3. $\langle x, x\rangle \in \mathrm{GF}(\sqrt{q})$.

We observe that the canonical basis B of $\mathrm{GF}(q)^l$ over $\mathrm{GF}(q)$ is *orthonormal* with respect to $\langle \cdot, \cdot \rangle$ ($\langle e, e'\rangle = 0$ if $e \neq e'$, and $\langle e, e\rangle = 1$ for all $e, e' \in B$), and it is clear that for every $x \in \mathrm{GF}(q)^l$, $x = \sum_{e \in B} \langle x, e\rangle e$. Nevertheless, contrary to the usual Hermitian situation, it may happen that for a non-zero vector $x \in \mathrm{GF}(q)^l$, $\langle x, x\rangle = 0$ (for instance, consider the situation where $q = 2^{2n}$, and $l = 2m$). But this dot product is *non-degenerate*: let us assume that for some x, $\langle x, y\rangle = 0$ for every y, then $x = (\underbrace{0, \ldots, 0}_{l \text{ factors}})$ (to see this it suffices to let y run over the canonical

basis of $\mathrm{GF}(q)^l$). Similarly, by conjugate symmetry, $\langle x, y\rangle = 0$ for each x implies that $y = (\underbrace{0, \ldots, 0}_{l \text{ factors}})$. Therefore, $\langle \cdot, \cdot \rangle$ defines a *pairing* (see [4]).

We denote $\mathrm{norm}_l(x) = \langle x, x\rangle = \sum_{i=1}^{l} \mathrm{norm}(x)$ for $x \in \mathrm{GF}(q)^l$, and finally $\mathcal{S}(\mathrm{GF}(q)^l)$ is defined as the hypersphere in $\mathrm{GF}(q)^l$ with center at $(\underbrace{0, \ldots, 0}_{l \text{ factors}})$ and radius 1.

4. Characters of certain finite Abelian groups over a finite field

Before beginning some formal developments, one should warn the reader on the limitations of the expected character theory in finite fields. In section 3, we claimed that $\mathcal{S}(\mathrm{GF}(q))$ is a cyclic group of order $\sqrt{q}+1$. Then for each nonzero integer d that divides $\sqrt{q}+1$, there is a (cyclic) subgroup of $\mathcal{S}(\mathrm{GF}(q))$ of order d, and this is the unique kind of subgroups. As a character theory is essentially used to faithfully represent an abstract group as an isomorphic group of functions, a copy of such group must be contained in the corresponding unit circle. Then our character theory in $\mathrm{GF}(q)$ will only apply on groups for which all their factors in a representation as a product direct group of cyclic subgroups divides $\sqrt{q}+1$.

Assumption 2. From now on d always denotes an element of $\mathbb{N}^*$ that divides $\sqrt{q}+1$.

Definition 4.1. (and proposition) The (cyclic) subgroup of $\mathcal{S}(\mathrm{GF}(q))$ of order d is denoted by $\mathcal{S}_d(\mathrm{GF}(q))$. In particular, $\mathcal{S}(\mathrm{GF}(q)) = \mathcal{S}_{\sqrt{q}+1}(\mathrm{GF}(q))$. If u is a generator of $\mathcal{S}(\mathrm{GF}(q))$ then $u^{\frac{\sqrt{q}+1}{d}}$ is a generator of $\mathcal{S}_d(\mathrm{GF}(q))$.

A *character* of a finite Abelian group G *with respect to* $\mathrm{GF}(q)$ (or simply a *character*) is a group homomorphism from G to $\mathcal{S}(\mathrm{GF}(q))$. Since a character χ is $\mathcal{S}(\mathrm{GF}(q))$-valued, $\chi(-x) = (\chi(x))^{-1} = \overline{\chi(x)}$, $\mathrm{norm}(\chi(x)) = 1$ and $\chi(0_G) = 1$ for each $x \in G$. By analogy with the traditional version, we denote by $\widehat{G}$ the set of all characters of G that we call its *dual*. When equipped with the point-wise multiplication, $\widehat{G}$ is a finite Abelian group. One recall that this multiplication is defined as

$$\forall \chi, \chi' \in \widehat{G},\ \chi\chi' \colon x \mapsto \chi(x)\chi'(x)\ . \tag{16}$$

As already mentionned in introduction, we focus on a very special kind of finite Abelian groups: the additive group of modulo d integers $\mathbb{Z}_d$ which is identified with the subset $\{0, \ldots, d-1\}$ of $\mathbb{Z}$.

Theorem 4.2. *The groups $\mathbb{Z}_d$ and $\widehat{\mathbb{Z}_d}$ are isomorphic.*

Proof. The parameter d has been chosen so that it divides $\sqrt{q}+1$. Then there is a unique (cyclic) subgroup $\mathcal{S}_d(\mathrm{GF}(q))$ of $\mathcal{S}(\mathrm{GF}(q))$ of order d. Let u_d be a generator of this group. Then the elements of $\widehat{\mathbb{Z}_d}$ have the form, for $j \in \mathbb{Z}_d$,

$$\chi_j \colon \left\{ \begin{array}{ccc} \mathbb{Z}_d & \to & \mathcal{S}_d(\mathrm{GF}(q)) \\ k & \mapsto & (u_d^j)^k = u_d^{jk}. \end{array} \right. \tag{17}$$

Actually the characters are $\mathcal{S}_d(\mathrm{GF}(q))$-valued since for each $x \in \mathbb{Z}_d$ and each character χ, $\chi(x) \in \mathcal{S}(\mathrm{GF}(q))$ by definition, and satisfies $1 = \chi(0) = \chi(dx) = (\chi(x))^d$

and then $\chi(x)$ is a d-th root of the unity. Then to determine a character $\chi \in \widehat{\mathbb{Z}_d}$, we need to compute the value of $\chi(k) = \chi(k1)$ for $k \in \{0, \ldots, d-1\}$, which gives

$$\chi(k) = u_d^{jk} \ . \tag{18}$$

In this equality, we have denoted $\chi(1)$ by u_d^j for $j \in \{0, \ldots, d-1\}$ since $\chi(1)$ is a d-th root of the unity in $\mathcal{S}(\mathrm{GF}(q))$. Then the character χ belongs to $\{\chi_0, \ldots, \chi_{d-1}\}$. Conversely, we observe that for $j \in \{1, \ldots, d-1\}$, the maps χ_j are group homomorphisms from $\mathbb{Z}_d$ to $\mathcal{S}(\mathrm{GF}(q))$ so they are elements of $\widehat{\mathbb{Z}_d}$. Let us define the following function.

$$\begin{array}{rccc} \Psi: & \mathbb{Z}_d & \to & \widehat{\mathbb{Z}_d} \\ & j & \mapsto & \chi_j \ . \end{array} \tag{19}$$

We have already seen that it is onto. Moreover, it is also one-to-one (it is sufficient to evaluate $\chi_j = \Psi(j)$ at 1) and it is obviously a group homomorphism. It is then an isomorphism, so that $\widehat{\mathbb{Z}_d}$ is isomorphic to $\mathbb{Z}_d$. □

The isomorphism established in theorem 4.2 between a group and its dual can be generalized as follows.

Proposition 3. *$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ and $(\widehat{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}})$ are isomorphic.*

Proof. The proof is easy since it is sufficient to remark that $(\widehat{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}})$ and $\widehat{\mathbb{Z}_{d_1}} \times \widehat{\mathbb{Z}_{d_2}}$ are isomorphic. We recall that d_1 and d_2 are both assumed to divide $\sqrt{q}+1$, thus $\widehat{\mathbb{Z}_{d_1}}$ and $\widehat{\mathbb{Z}_{d_2}}$ exist and are isomorphic to $\mathbb{Z}_{d_1}$ and $\mathbb{Z}_{d_2}$ respectively. Let i_1 be the first canonical injection of $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ and i_2 the second (when $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ is seen as a direct sum). The following map

$$\Phi: \left\{ \begin{array}{lcl} (\widehat{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}}) & \to & \widehat{\mathbb{Z}_{d_1}} \times \widehat{\mathbb{Z}_{d_2}} \\ \chi & \mapsto & (\chi \circ i_1, \chi \circ i_2) \end{array} \right. \tag{20}$$

is a group isomorphism. It is obviously one-to-one and for $(\chi_1, \chi_2) \in \widehat{\mathbb{Z}_{d_1}} \times \widehat{\mathbb{Z}_{d_2}}$, the map $\chi : (x_1, x_2) \mapsto \chi_1(x_1)\chi_2(x_2)$ is an element of $(\widehat{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}})$ and $\Phi(\chi) = (\chi_1, \chi_2)$. Then $(\widehat{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}})$ is isomorphic to $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ since $\widehat{Z_{d_i}}$ and $\mathbb{Z}_{d_i}$ are isomorphic (for $i = 1, 2$). □

From proposition 3 it follows in particular that $\widehat{\mathbb{Z}_d^m}$ is isomorphic to $\mathbb{Z}_d^m$. This result also provides a specific form to the characters of $\mathbb{Z}_d^m$ as follows. We define a dot product, which is a $\mathbb{Z}_d$-bilinear map from $(\mathbb{Z}_d^m)^2$ to $\mathbb{Z}_d$, by

$$x \cdot y = \sum_{i=1}^{m} x_i y_i \in \mathbb{Z}_d \tag{21}$$

for $x, y \in \mathbb{Z}_d^m$. Then the character that corresponds to $\alpha \in \mathbb{Z}_d^m$ can be defined by

$$\begin{array}{rccc} \chi_\alpha: & \mathbb{Z}_d^m & \to & \mathcal{S}_d(\mathrm{GF}(q)) \\ & x & \mapsto & u_d^{\alpha \cdot x} \end{array} \tag{22}$$

where u_d is a generator of $\mathcal{S}_d(\mathrm{GF}(q))$. In particular for each $\alpha, x \in \mathbb{Z}_d^m$, $\chi_\alpha(x) = \chi_x(\alpha)$. The following result is obvious.

Corollary 1. *Let $G \cong \prod_{i=1}^{N} \mathbb{Z}_{d_i}^{m_i}$ be a finite Abelian group for which each integer d_i divides $\sqrt{q}+1$. Then G and $\widehat{G}$ are isomorphic.*

Remark 1. The fact that $G \cong \widehat{G}$ does not depend on a decomposition of G into a direct sum of cyclic groups. But a particular isomorphism of corollary 1 depends on the decomposition $\prod_{i=1}^{N} \mathbb{Z}_{d_i}^{m_i}$ of the group G.

If $G = \prod_{i=1}^{N} \mathbb{Z}_{d_i}^{m_i}$ satisfies the assumption of the corollary 1, then we can also obtain a specific form for its characters and a specific isomorphism from G to its dual. Let $\alpha = (\alpha_1, \ldots, \alpha_N) \in G$.

$$\begin{array}{rccc} \chi_\alpha \colon & G & \to & \mathcal{S}(\mathrm{GF}(q)) \\ & x = (x_1, \ldots, x_N) & \mapsto & \prod_{i=1}^{N} u_{d_i}^{\alpha_i \cdot x_i} \end{array} \tag{23}$$

where for each $i \in \{1, \ldots, N\}$, u_{d_i} is a generator of $\mathcal{S}_{d_i}(\mathrm{GF}(q))$. In particular for each $\alpha, x \in G^2$, we also have $\chi_\alpha(x) = \chi_x(\alpha)$.

Assumption 3. From now on, each finite Abelian group G considered is assumed to be of a specific form $\prod_{i=1}^{N} \mathbb{Z}_{d_i}^{m_i}$ where for each $i \in \{1, \ldots, N\}$, d_i divides $\sqrt{q}+1$, so that we have at our disposal a specific isomorphism given by the formula (23) between G and $\widehat{G}$.

The dual $\widehat{G}$ of G is constructed and is shown to be isomorphic to G. We may also be interested into the *bidual* $\widehat{\widehat{G}}$ of G, namely the dual of $\widehat{G}$. Similarly to the usual situation of complex-valued characters, we prove that G and its bidual are canonically isomorphic. It is already clear that $G \cong \widehat{\widehat{G}}$ (because $G \cong \widehat{G}$ and $\widehat{G} \cong \widehat{\widehat{G}}$). But this isomorphism is far from being canonical since it depends on a decomposition of G, and of $\widehat{G}$, and choices for generators of each cyclic factor in the given decomposition. We observe that the map $e \colon G \to \widehat{\widehat{G}}$ defined by $e(x)(\chi) = \chi(x)$ for every $x \in G$, $\chi \in \widehat{G}$ is a group homomorphism. To prove that it is an isomorphism it suffices to check that e is one-to-one (since G and $\widehat{\widehat{G}}$ have the same order). Let $x \in \ker(e)$. Then, for all $\chi \in \widehat{G}$, $\chi(x) = 1$. Let us fix an isomorphism $\alpha \in G \to \chi_\alpha \in \widehat{G}$ as in the formula (23). Then, for every $\alpha \in G$, $\chi_\alpha(x) = 1 = \chi_x(\alpha)$ so that $x = 0_G$. Thus we have obtained an appropriate version of Pontryagin-van Kampen duality (see [10]). Let us recall that according to the *structure theorem of finite Abelian groups*, for any finite Abelian group G, there is a unique finite sequence of positive integers, called the *invariants of* G, $d_1, \cdots, d_{\ell_G}$ such that d_i divides d_{i+1} for each $i < \ell_G$. Let us denote by $\mathcal{Ab}_{\sqrt{q}+1}$ the category of all finite Abelian groups G such that d_{ℓ_G} divides $\sqrt{q}+1$, with usual homomorphisms of groups as arrows. From the previous results, if G is an object of $\mathcal{Ab}_{\sqrt{q}+1}$, then $G \cong \widehat{G}$. Moreover, $\widehat{(\cdot)}$ defines a contravariant functor (see [15]) from $\mathcal{Ab}_{\sqrt{q}+1}$ to itself. Indeed, if $\phi \colon G \to H$ is a homomorphism of groups (where G, H belongs to

$\mathcal{Ab}_{\sqrt{q}+1}$), then $\widehat{\phi}\colon \widehat{H} \to \widehat{G}$ defined by $\widehat{\phi}(\chi) = \chi \circ \phi$ is a homomorphism of groups. Then, we have the following duality theorem.

Theorem 4.3 (Duality)**.** *The covariant (endo-)functor* $\widehat{\widehat{(\cdot)}}\colon \mathcal{Ab}_{\sqrt{q}+1} \to \mathcal{Ab}_{\sqrt{q}+1}$ *is a (functorial) isomorphism (this means in particular that* $G \cong \widehat{\widehat{G}}$*).*

5. Orthogonality relations

The characters satisfy a certain kind of orthogonality relation. In order to establish it we introduce the natural "action" of $\mathbb{Z}$ on any finite field $\mathrm{GF}(p^l)$ of characteristic p as $kx = x\underbrace{+\ldots+}_{k\ times}x$ for $(k, x) \in \mathbb{Z} \times \mathrm{GF}(p^l)$. This is nothing else than the fact that the underlying Abelian group structure of $\mathrm{GF}(p^l)$ is a $\mathbb{Z}$-module. In particular one has for each $(k, k', x) \in \mathbb{Z} \times \mathbb{Z} \times \mathrm{GF}(p^l)$,

1. $0x = 0$, $1x = x$ and $k0 = 0$,
2. $(k + k')x = kx + k'x$ and then $nkx = n(kx)$,
3. $k1 \in \mathrm{GF}(p)$, $k1 = (k \bmod p)1$, $k^m 1 = (k1)^m$ and if $k \bmod p \neq 0$, then $(k1)^{-1} = (k \bmod p)^{-1}1$.

In the remainder we identify $k1$ with $k \bmod p$ or in other terms we make an explicit identification of $\mathrm{GF}(p)$ by $\mathbb{Z}_p$.

Lemma 5.1. *Let G be a finite Abelian group. For $\chi \in \widehat{G}$,*

$$\sum_{x\in G} \chi(x) = \begin{cases} 0 & \text{if } \chi \neq 1\ , \\ (|G| \bmod p) & \text{if } \chi = 1\ . \end{cases} \tag{24}$$

Proof. If $\chi = 1$, then $\displaystyle\sum_{x\in G} 1 = (|G| \bmod p)$ since the characteristic of $\mathrm{GF}(q)$ is equal to p. Let us suppose that $\chi \neq 1$. Let $x_0 \in G$ such that $\chi(x_0) \neq 1$. Then we have

$$\chi(x_0) \sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(x_0 + x) = \sum_{y\in G} \chi(y), \tag{25}$$

so that $(\chi(x_0) - 1) \displaystyle\sum_{x\in G} \chi(x) = 0$ and thus $\displaystyle\sum_{x\in G} \chi(x) = 0$ (because $\chi(x_0) \neq 1$). □

This technical lemma allows us to define the orthogonality relation between characters.

Definition 5.2. Let G be a finite Abelian group. Let $f, g \in \mathrm{GF}(q)^G$. We define the "inner product" of f and g by

$$\langle f, g\rangle = \sum_{x\in G} f(x)\overline{g(x)} \in \mathrm{GF}(q). \tag{26}$$

The above definition does not ensure that $\langle f, f\rangle = 0$ implies that $f \equiv 0$ as it holds for a true inner product. Indeed, take $q = 2^{2n}$, and let $f\colon \mathbb{Z}_2 \to \mathrm{GF}(2^{2n})$ be the constant map with value 1. Then, $\langle f, f\rangle = 0$. Thus, contrary to a usual Hermitian dot product, an orthogonal family (with respect to $\langle\cdot,\cdot\rangle$) of $\mathrm{GF}(q)^G$ is not necessarily $\mathrm{GF}(q)$-linearly independent.

Proposition 4 (Orthogonality relation)**.** *Let G be a finite Abelian group. For all $(\chi_1, \chi_2) \in \widehat{G}^2$ then*

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2, \\ |G| \bmod p & \text{if } \chi_1 = \chi_2. \end{cases} \tag{27}$$

Proof. Let us denote $\chi = \chi_1 \chi_2^{-1} = \chi_1 \overline{\chi_2}$. We have:

$$\langle \chi_1, \chi_2 \rangle = \sum_{x \in G} \chi(x). \tag{28}$$

If $\chi_1 = \chi_2$, then $\chi = 1$ and if $\chi_1 \neq \chi_2$, then $\chi \neq 1$. The proof is obtained by using the previous lemma 5.1. □

Remark 2. The term *orthogonality* would be abusive if $|G| \bmod p = 0$, because then $\sum_{x \in G} \chi(x) = 0$ for all $\chi \in \widehat{G}$. Nevertheless we know from the assumption 3 that all the d_i's divide $\sqrt{q} + 1 = p^n + 1$. In particular, $d_i = 1 \bmod p$ and therefore $|G| = \prod_i d_i^{m_i}$ is co-prime to p, and the above situation cannot occur, so $|G|$ is invertible modulo p.

6. Fourier transform over a finite field

In this section is developed a Fourier transform for functions defined on G and based on the theory of characters introduced in section 4. There is already a Fourier transform with values in some finite field called *Mattson-Solomon transform* [3] but it maps a function $f \in \mathrm{GF}(q)^{\mathbb{Z}_d}$ to a function $g \in \mathrm{GF}(q^m)^{\mathbb{Z}_d}$ where m is the smallest positive integer so that d divides $q^m - 1$. In this paper we want our Fourier transform to "live" in a finite field $\mathrm{GF}(q)$ and not in one of its extensions. Moreover the existing transform is not based on an explicit Hermitian structure nor on a theory of characters. For these reasons, we need to introduce a new kind of Fourier transform.

Let u be a generator of $\mathcal{S}(\mathrm{GF}(q))$. Let G be a finite Abelian group and $f : G \to \mathrm{GF}(q)$. We define the following function.

$$\begin{array}{rccc} \widehat{f}\colon & \widehat{G} & \longrightarrow & \mathrm{GF}(q) \\ & \chi & \mapsto & \displaystyle\sum_{x \in G} f(x)\chi(x)\ . \end{array} \tag{29}$$

Remark 3. We warm the reader that we use the same notation $\widehat{f}$ as the one used for the Fourier transform of a complex-valued function. From now on only the second definition is used.

Because $G = \prod_{i=1}^{N} \mathbb{Z}_{d_i}^{m_i}$, by using the isomorphism between G and its dual group from section 4, we can define

$$\begin{array}{rccc} \widehat{f}\,\colon & G & \longrightarrow & \mathrm{GF}(q) \\ & \alpha & \mapsto & \displaystyle\sum_{x \in G} f(x)\chi_\alpha(x) = \sum_{x \in G} f(x) \prod_{i=1}^{N} u^{\frac{(\sqrt{q}+1)\alpha_i \cdot x_i}{d_i}} \end{array} \tag{30}$$

Let us compute $\widehat{\widehat{f}}$. Let $\alpha \in G$. We have

$$\begin{aligned}
\widehat{\widehat{f}}(\alpha) &= \sum_{x\in G} \widehat{f}(x)\chi_\alpha(x) \\
&= \sum_{x\in G}\sum_{y\in G} f(y)\chi_x(y)\chi_\alpha(x) \\
&= \sum_{x\in G}\sum_{y\in G} f(y)\chi_y(x)\chi_\alpha(x) \\
&= \sum_{y\in G} f(y) \sum_{x\in G} \chi_{\alpha+y}(x) \\
&= (|G| \bmod p) f(-\alpha)
\end{aligned} \tag{31}$$

The last equality holds since

$$\sum_{x\in G} \chi_{\alpha+y}(x) = \begin{cases} 0 & \text{if } y \neq -\alpha \ , \\ (|G| \bmod p) & \text{if } y = -\alpha \ . \end{cases}$$

Now if we assume that $(|G| \bmod p) = 0$, then it follows that the function $f \mapsto \widehat{f}$ is non invertible but this situation cannot occur since from the assumption 3, $|G|$ is invertible modulo p. Therefore we can claim that the function $\widehat{(\cdot)}$ that maps $f \in \mathrm{GF}(q)^G$ to $\widehat{f} \in \mathrm{GF}(q)^G$ is invertible. It is referred to as the *Fourier transform* of f (with respect to $\mathrm{GF}(q)$) and it admits an *inversion formula*: for $f \in \mathrm{GF}(q)^G$ and for each $x \in G$,

$$f(x) = (|G| \bmod p)^{-1} \sum_{\alpha\in G} \widehat{f}(\alpha)\overline{\chi_\alpha(x)} \tag{32}$$

where $(|G| \bmod p)^{-1}$ is the multiplicative inverse of $(|G| \bmod p)$ in $\mathbb{Z}_p$ (this inverse exists according to the choice of G). This Fourier transform shares many properties with the classical discrete Fourier transform.

Definition 6.1. Let G be a finite Abelian group. Let $f, g \in \mathrm{GF}(q)^G$. For each $\alpha \in G$, we define the *convolutional product* of f and g at α by

$$(f * g)(\alpha) = \sum_{x\in G} f(x)g(-x+\alpha) \ . \tag{33}$$

Proposition 5 (Trivialization of the convolutional product)**.** *Let $f, g \in \mathrm{GF}(q)^G$. For each $\alpha \in G$,*

$$\widehat{(f * g)}(\alpha) = \widehat{f}(\alpha)\widehat{g}(\alpha) \ . \tag{34}$$

Proof. Let $\alpha \in G$. We have

$$\begin{aligned}
\widehat{(f * g)}(\alpha) &= \sum_{x\in G} (f * g)(x)\chi_\alpha(x) \\
&= \sum_{x\in G}\sum_{y\in G} f(y)g(-y+x)\chi_\alpha(x) \\
&= \sum_{x\in G}\sum_{y\in G} f(y)g(-y+x)\chi_\alpha(y-y+x) \\
&= \sum_{x\in G}\sum_{y\in G} f(y)g(-y+x)\chi_\alpha(y)\chi_\alpha(-y+x) \\
&= \widehat{f}(\alpha)\widehat{g}(\alpha) \ .
\end{aligned} \tag{35}$$

□

We recall that the group-algebra $\mathrm{GF}(q)[G]$ of G over $\mathrm{GF}(q)$ is the $\mathrm{GF}(q)$-vector space $\mathrm{GF}(q)^G$ with point-wise addition, and with the convolution product. We observe that the Fourier transform $\widehat{(\cdot)}$ is an algebra isomorphism from the group-algebra $\mathrm{GF}(q)[G]$ of G its usual convolution product to $\mathrm{GF}(q)[G]$ with the point-wise product. Moreover, let $(\delta_x)_{x\in G}$ be the canonical basis of $\mathrm{GF}(q)^G$ (as a $\mathrm{GF}(q)$-vector space), that is, $\delta_x(y) = 0$ if $x \neq y$ and $\delta_x(x) = 1$. It is easy to see (using a fixed isomorphism between G and $\widehat{G}$) that $\widehat{\delta}_x = \chi_x$. Because $\widehat{(\cdot)}$ is an isomorphism, this means that $(\chi_x)_{x\in G}$ is a basis of $\mathrm{GF}(q)^G$ over $\mathrm{GF}(q)$, and it turns that the Fourier transform $\widehat{f}$ of $f \in \mathrm{GF}(q)^G$ is the decomposition of f into the basis of characters (we recall here that the fact for a family of elements of $\mathrm{GF}(q)^G$ to be orthogonal with respect to the inner-product $\langle\cdot,\cdot\rangle$ of $\mathrm{GF}(q)^G$ does not ensure that the family into consideration is linearly independent because $\langle\cdot,\cdot\rangle$ is not positive-definite).

We continue to enunciate formulas obtained by considering the decomposition into the basis of characters.

Proposition 6 (Plancherel formula)**.** *Let $f, g \in \mathrm{GF}(q)^G$. Then,*

$$\sum_{x\in G} f(x)\overline{g(x)} = (|G| \bmod p)^{-1} \sum_{\alpha\in G} \widehat{f}(\alpha)\overline{\widehat{g}(\alpha)} \ . \tag{36}$$

Proof. Let us define the following functions for any finite group G and any function $h : G \to \mathrm{GF}(q)$,

$$\begin{array}{lllll} I_G\colon & G & \to & G \\ & x & \mapsto & -x \\ & \text{and} & & \\ \overline{h}\colon & G & \to & \mathrm{GF}(q) \\ & x & \mapsto & \overline{h(x)} \ . \end{array} \tag{37}$$

Then we have $(f * \overline{g} \circ I_G)(0_G) = \sum_{x\in G} f(x)\overline{g(x)}$. But from the inversion formula we have also

$$\begin{array}{rcl} (f * \overline{g} \circ I_G)(0_G) & = & (|G| \bmod p)^{-1} \sum_{\alpha\in G} \widehat{(f * \overline{g} \circ I_G)}(\alpha) \\ & = & (|G| \bmod p)^{-1} \sum_{\alpha\in G} \widehat{f}(\alpha)\widehat{(\overline{g} \circ I_G)}(\alpha) \\ & & \text{(by the trivialization of the convolutional product.)} \end{array} \tag{38}$$

Let us compute $\widehat{(\overline{g} \circ I_G)}(\alpha)$ for $\alpha \in G$.

$$\begin{aligned}
\widehat{(\overline{g} \circ I_G)}(\alpha) &= \sum_{x \in G} (\overline{g} \circ I_G)(x) \chi_\alpha(x) \\
&= \sum_{x \in G} \overline{g(-x)} \chi_\alpha(x) \\
&= \sum_{x \in G} \overline{g(x)} \chi_\alpha(-x) \\
&= \sum_{x \in G} \overline{g(x)} (\chi_\alpha(x))^{-1} \\
&= \sum_{x \in G} \overline{g(x) \chi_\alpha(x)} \\
&= \overline{\sum_{x \in G} g(x) \chi_\alpha(x)} \\
&= \overline{\widehat{g}(\alpha)} \ .
\end{aligned} \tag{39}$$

Then we obtain the equality

$$(f * \overline{g} \circ I_G) = (|G| \bmod p)^{-1} \sum_{\alpha \in G} \widehat{f}(\alpha) \overline{\widehat{g}(\alpha)} \tag{40}$$

that ensures the correct result. □

Corollary 2 (Parseval equation)**.** *Let $f, g \in \mathrm{GF}(q)^G$. Then*

$$\sum_{x \in G} \mathrm{norm}(f(x)) = (|G| \bmod p)^{-1} \sum_{\alpha \in G} \mathrm{norm}(\widehat{f}(\alpha)) \ . \tag{41}$$

In particular, if f is $\mathcal{S}(\mathrm{GF}(q))$-valued, then

$$\sum_{\alpha \in G} \mathrm{norm}(\widehat{f}(\alpha)) = (|G| \bmod p)^2 \ . \tag{42}$$

Proof. It is sufficient to apply Plancherel formula with $g = f$. □

7. Bent functions over a finite field

Up to now, the following ingredients have been introduced: an Hermitian-like structure on degree two extensions, a finite-field character theory for finite Abelian groups (of order co-prime to the characteristic), and a corresponding Fourier transform. All of them may be constituents of a bentness-like notion in this particular setting. As already explained in introduction, although we are aware of an existing notion of bent functions in finite fields [1], in this contribution we do not make any interesting connections with these maps and those introduced below, except that they share very similar properties. Nevertheless, we compare the notion of bentess due to Logachev, Salnikov and Yashchenko in [12] to our, and we prove that many bent functions as defined in [12] are also bent functions in our setting. The notion of bentness introduced now serves also as an illustration of our character theory. In this section we also prove the existence of functions which are bent in a sense presented hereafter.

In the traditional setting, *i.e.*, for complex-valued functions defined on any finite Abelian group G, bent functions [6, 8, 12, 16, 18] are those maps $f\colon G \to \mathcal{S}(\mathbb{C})$ such that for each $\alpha \in G$,

$$|\widehat{f}(\alpha)|^2 = |G| \ . \tag{43}$$

This notion is closely related to some famous cryptanalysis namely the differential [2] and linear [13] attacks on secret-key cryptosystems. We translate this concept in the current finite-field setting as follows.

Definition 7.1. The map $f\colon G \to \mathcal{S}(\mathrm{GF}(q))$ is called bent if for all $\alpha \in G$,

$$\mathrm{norm}(\widehat{f}(\alpha)) = (|G| \bmod p) \ . \tag{44}$$

7.1. Derivative and bentness

In the traditional approach the relation with bentness and differential attack is due to the following result.

Proposition 7. *[12] Let $f\colon G \to \mathcal{S}(\mathbb{C})$. The function f is bent if, and only if, for all $\alpha \in G^*$,*

$$\sum_{x \in G} f(\alpha + x)\overline{f(x)} = 0 \ . \tag{45}$$

Similarly, it is possible to characterize the new concept of bentness in a similar way. Let $f\colon G \to \mathrm{GF}(q)$. For each $\alpha \in G$, we define the *derivative of f in direction α* as

$$\begin{array}{rccc} d_\alpha f\colon & G & \to & \mathrm{GF}(q) \\ & x & \mapsto & f(\alpha + x)\overline{f(x)} \ . \end{array} \tag{46}$$

Lemma 7.2. *Let $f\colon G \to \mathrm{GF}(q)$. We have*

1. $\forall x \in G^*,\ f(x) = 0 \Leftrightarrow \forall \alpha \in G,\ \widehat{f}(\alpha) = f(0_G)$.
2. $\forall \alpha \in G^*,\ \widehat{f}(\alpha) = 0 \Leftrightarrow f$ *is constant.*

Proof. 1.

$\Rightarrow)$ $\widehat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x) = f(0_G)\chi_\alpha(0_G) = f(0_G)$,

$\Leftarrow)$ According to the inversion formula,

$$\begin{array}{rcl} f(x) & = & (|G| \bmod p)^{-1} \sum_{\alpha \in G} \widehat{f}(\alpha)\overline{\chi_\alpha(x)} \\ & = & f(0_G)(|G| \bmod p)^{-1} \sum_{\alpha \in G} \chi_{-x}(\alpha) \\ & = & 0 \text{ for all } x \neq 0_G \ . \end{array} \tag{47}$$

2.

$\Rightarrow)$ $f(x) = (|G| \bmod p)^{-1} \sum_{\alpha \in G} \widehat{f}(\alpha)\overline{\chi_\alpha(x)} = \widehat{f}(0_G)(|G| \bmod p)^{-1}$,

$\Leftarrow)$ $\widehat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x) = \textit{constant} \sum_{x \in G} \chi_\alpha(x) = 0$ for all $\alpha \neq 0_G$.

□

Lemma 7.3. *Let $f\colon G \to \mathrm{GF}(q)$. We define the autocorrelation function of f as*

$$\begin{array}{rccc} AC_f\colon & G & \to & \mathrm{GF}(q) \\ & \alpha & \mapsto & \displaystyle\sum_{x\in G} d_\alpha f(x)\ . \end{array} \tag{48}$$

Then, for all $\alpha \in G$, $\widehat{AC_f}(\alpha) = \mathrm{norm}(\widehat{f}(\alpha))$.

Proof. Let $\alpha \in G$.

$$\begin{array}{rcl} \widehat{AC_f}(\alpha) & = & \displaystyle\sum_{x\in G} AC_f(x)\chi_\alpha(x) \\ & = & \displaystyle\sum_{x\in G}\sum_{y\in G} d_x f(y)\chi_\alpha(x) \\ & = & \displaystyle\sum_{x\in G}\sum_{y\in G} f(xy)\overline{f(y)}\chi_\alpha(xy)\overline{\chi_\alpha(y)} \\ & = & \widehat{f}(\alpha)\overline{\widehat{f}(\alpha)} \\ & = & \mathrm{norm}(\widehat{f}(\alpha))\ . \end{array} \tag{49}$$

□

We use the above results to obtain the following characterization of bentness as a combinatorial object using the derivative.

Theorem 7.4. *The function $f : G \to \mathcal{S}(\mathrm{GF}(q))$ is bent if, and only if, for all $\alpha \in G^*$, $\displaystyle\sum_{x\in G} d_\alpha f(x) = 0$.*

Proof. $\forall \alpha \in G^*,\ \displaystyle\sum_{x\in G} d_\alpha f(x) = 0$
$\Leftrightarrow \forall \alpha \in G^*,\ AC_f(\alpha) = 0$
$\Leftrightarrow \forall \alpha \in G,\ \widehat{AC_f}(\alpha) = AC_f(0_G)$
(according to lemma 7.2)
$\Leftrightarrow \forall \alpha \in G,\ \mathrm{norm}(\widehat{f}(\alpha)) = \displaystyle\sum_{x\in G} f(x)\overline{f(x)}$
(according to lemma 7.3)
$\Leftrightarrow \forall \alpha \in G,\ \mathrm{norm}(\widehat{f}(\alpha)) = \displaystyle\sum_{x\in G} \mathrm{norm}(f(x))$
$\Leftrightarrow \forall \alpha \in G,\ \mathrm{norm}(\widehat{f}(\alpha)) = (|G| \bmod p)$
(because f is $\mathcal{S}(\mathrm{GF}(q))$-valued.) □

7.2. Comparison between the two bentness notions

In what follows we refer to the traditional bent functions, as introduced in the beginning of section 7, as "bent in the usual sense", while our own bent functions (definition 7.1) are referred to as "bent in the finite-field sense". In this subsection we prove that any bent "well-behaved" function in the usual sense is also a bent function in the finite-field sense.

Let $\mathbb{U}_m$ be the group of complex m-th roots of unity. Let us assume that m that divides $\sqrt{q}+1$. Therefore, $\mathbb{U}_m$ may be identified with the (unique) sub-group

of $\mathcal{S}(\mathrm{GF}(q))$ of order m. We also remark that for every $\omega \in \mathbb{U}_m$, the complex-conjugate $\overline{\omega} = \omega^{-1}$, and if the same ω is seen as an element of $\mathcal{S}(\mathrm{GF}(q))$, then also $\omega^{\sqrt{q}} = \omega^{-1}$. Conversely, any sub-group of $\mathcal{S}(\mathrm{GF}(q))$ may be identified with a sub-group of $\mathbb{U}_{\sqrt{q}+1}$. Let us assume that G belongs to $\mathcal{Ab}_{\sqrt{q}+1}$. Let us denote by $\widetilde{G}$ the group of complex-valued characters of G. We have $\widetilde{G} \cong G \cong \widehat{G}$. It is clear that any complex-valued character of G takes its values in $\mathbb{U}_{\sqrt{q}+1} \cong \mathcal{S}(\mathrm{GF}(q))$. So that for every $x \in G$, and every $\chi \in \widetilde{G} \cong \widehat{G}$, $f(x)\chi(x) \in \mathbb{U}_{\sqrt{q}+1} \cong \mathcal{S}(\mathrm{GF}(q))$. Let $\mathbb{Z}[\mathbb{U}_{\sqrt{q}+1}]$ be the group-ring of $\mathbb{U}_{\sqrt{q}+1}$, and let $\overline{\mathbb{U}}_{\sqrt{q}+1}$ be the sub-ring of $\mathbb{C}$ generated by $\mathbb{U}_{\sqrt{q}+1}$. Let $\pi\colon \mathbb{Z}[\mathbb{U}_{\sqrt{q}+1}] \to \overline{\mathbb{U}}_{\sqrt{q}+1}$ be the unique ring homomorphism such that $\pi([\omega]) = \omega$ for all $\omega \in \mathbb{U}_{\sqrt{q}+1}$ (where $[\cdot]\colon \mathbb{U}_{\sqrt{q}+1} \to \mathbb{Z}[\mathbb{U}_{\sqrt{q}+1}]$ is the canonical inclusion). It is clear that as rings $\overline{\mathbb{U}}_{\sqrt{q}+1} \cong \mathbb{Z}[\mathbb{U}_{\sqrt{q}+1}]/\ker(\pi)$. Similarly, let $\phi\colon \mathbb{Z}[\mathbb{U}_{\sqrt{q}+1}] \to \mathrm{GF}(q)$ be the unique ring homomorphism such that $\phi([\omega]) = \tilde{\omega}$ for every $\omega \in \mathbb{U}_{\sqrt{q}+1}$ (where $\tilde{\omega}$ denotes the image of ω under an isomorphism $\mathbb{U}_{\sqrt{q}+1} \to \mathcal{S}(\mathrm{GF}(q))$). It is easily checked that $\ker(\pi) \subseteq \ker(\phi)$ so that ϕ passes to the quotient as a ring homomorphism $\phi_0\colon \overline{\mathbb{U}}_{\sqrt{q}+1} \to \mathrm{GF}(q)$ such that $\phi_0(\omega) = \tilde{\omega}$ for every $\omega \in \mathbb{U}_{\sqrt{q}+1}$ (we observe that the restriction of ϕ_0 to $\mathbb{U}_{\sqrt{q}+1}$ is precisely the isomorphism $\mathbb{U}_{\sqrt{q}+1} \to \mathcal{S}(\mathrm{GF}(q))$ chosen). We notice that for every integer n, $\phi_0(n\omega) = (n \bmod p)\tilde{\omega}$, and $\phi_0(\overline{\omega}) = (\tilde{\omega})^{\sqrt{q}} = \overline{\tilde{\omega}}$. Now, let us assume that $f\colon G \to \mathbb{U}_m$. Denoting its usual complex-valued Fourier transform by $\tilde{f}$, we have $\phi_0(\tilde{f}) = \widehat{f}$. Let us assume that f is bent (in the traditional meaning), *i.e.*, $|\tilde{f}(\alpha)|^2 = |G|$ for every $\alpha \in G$. This equivalent to $\tilde{f}(\alpha)\overline{\tilde{f}(\alpha)} = |G|$ for every $\alpha \in G$. Then, $\mathrm{norm}(\tilde{f}(\alpha)) = \phi_0(|G|) = |G| \bmod p$ for every $\alpha \in G$, so that f is bent in this finite-field setting. The following result is then proved.

Theorem 7.5. *Let m be a divisor of $\sqrt{q}+1$. Let G be a group in the category $\mathcal{Ab}_{\sqrt{q}+1}$. Let $f\colon G \to \mathbb{U}_m$. If f is bent in the usual sense, then it is also bent in the finite-field setting sense.*

This result motivates the study of such bent functions in the finite-field sense.

7.3. Dual bent function

Again by analogy to the traditional notion [7, 11], it is also possible to define a *dual* bent function from a given bent function. Actually, as we see it below, $|G|$ must be a square in $\mathrm{GF}(p)$ to ensure the well-definition of a dual bent. So by using the famous *law of quadratic reciprocity*, we can add the following requirement (which contrary to the other assumptions is only needed for proposition 8).

Assumption 4. If the prime number p is ≥ 3, then $|G|$ must also satisfy $|G|^{\frac{p-1}{2}} \equiv 1 \pmod p$. If the prime number $p = 2$, then there is no other assumptions on $|G|$ (than those already made).

According to assumption 4, $|G| \bmod p$ is a square in $\mathrm{GF}(p)$, then there is at least one $x \in \mathrm{GF}(p)$ with $x^2 = |G| \bmod p$. If $p = 2$, then $x = 1$. If $p \geq 3$, then we choose for x the element $(|G| \bmod p)^{\frac{p+1}{4}}$. Indeed it is a square root of $|G| \bmod p$ since $((|G| \bmod p)^{\frac{p+1}{4}})^2 = (|G| \bmod p)^{\frac{p+1}{2}} = (|G| \pmod p)(|G| \pmod p)^{\frac{p-1}{2}} = |G| \pmod p$. In all cases we denote by $(|G| \bmod p)^{\frac{1}{2}}$ the chosen square root of $|G| \bmod p$. Since $|G| \bmod p \neq 0$, then it is clear that this square root also is non-zero. Its inverse is denoted by $(|G| \bmod p)^{-\frac{1}{2}}$. Finally it is clear that $((|G| \bmod p)^{-\frac{1}{2}})^2 = (|G| \bmod p)^{-1}$.

Proposition 8. *Let $f\colon G \to \mathcal{S}(\mathrm{GF}(q))$ be a bent function, then the following function $\widetilde{f}$, called dual of f, is bent.*

$$\begin{array}{rccl} \widetilde{f}\colon & G & \to & \mathcal{S}(\mathrm{GF}(q)) \\ & \alpha & \mapsto & (|G| \bmod p)^{-\frac{1}{2}} \widehat{f}(\alpha)\ . \end{array} \tag{50}$$

Proof. Let us first check that $\widetilde{f}$ is $\mathcal{S}(\mathrm{GF}(q))$-valued. Let $\alpha \in G$. We have

$$\begin{array}{rcl} \widetilde{f}(\alpha)\overline{\widetilde{f}(\alpha)} & = & (|G| \bmod p)^{-\frac{1}{2}} \widehat{f}(\alpha)(|G| \bmod p)^{-\frac{1}{2}} \overline{\widehat{f}(\alpha)} \\ & = & (|G| \bmod p)^{-1} \mathrm{norm}(\widehat{f}(\alpha)) \\ & = & 1 \text{ (since } f \text{ is bent.)} \end{array} \tag{51}$$

Let us check that the bentness property holds for $\widetilde{f}$. Let $\alpha \in G$. We have $\widehat{\widetilde{f}}(\alpha) = (|G| \bmod p)^{-\frac{1}{2}}(|G| \bmod p) f(-\alpha)$ (according to formula (31)). Then

$$\begin{array}{rcl} \widehat{\widetilde{f}}(\alpha)\overline{\widehat{\widetilde{f}}(\alpha)} & = & (|G| \bmod p) f(-\alpha)\overline{f(-\alpha)} \\ & = & (|G| \bmod p) \mathrm{norm}(f(-\alpha)) \\ & = & (|G| \bmod p) \text{ (since } f \text{ is } \mathcal{S}(\mathrm{GF}(q))\text{-valued.)} \end{array} \tag{52}$$

□

7.4. Construction of bent functions

We present a construction which is actually the translation in our setting of a simple version of the well-known Maiorana-McFarland construction [8, 14] for classical bent functions.

Let $g\colon G \to \mathcal{S}(\mathrm{GF}(q))$ be any function. Let f be the following function.

$$\begin{array}{rccl} f\colon & G^2 & \to & \mathcal{S}(\mathrm{GF}(q)) \\ & (x, y) & \mapsto & \chi_x(y) g(y)\ . \end{array} \tag{53}$$

Then f is bent. We observe that the fact that f is $\mathcal{S}(\mathrm{GF}(q))$-valued is obvious by construction. So let us prove that f is indeed bent. We use the combinatorial characterization obtained in theorem 7.4. Let $\alpha, \beta, x, y \in G$. Then we have

$$\begin{array}{rcl} d_{(\alpha,\beta)} f(x, y) & = & f(\alpha + x, \beta + y)\overline{f(x, y)} \\ & = & \chi_{\alpha+x}(\beta + y) g(\beta + y)\overline{\chi_x(y)}\ \overline{g(y)} \\ & = & \chi_\alpha(\beta + y)\chi_x(\beta + y) g(\beta + y)\overline{\chi_x(y)}\ \overline{g(y)} \\ & = & \chi_\alpha(\beta)\chi_\alpha(y)\chi_x(\beta)\chi_x(y) g(\beta + y)\overline{\chi_x(y)}\ \overline{g(y)} \\ & = & \chi_\alpha(\beta)\chi_\alpha(y) g(\beta + y)\overline{g(y)}\chi_x(\beta) \\ & = & \chi_\alpha(\beta)\chi_\alpha(y) g(\beta + y)\overline{g(y)}\chi_\beta(x) \text{ (because } \chi_x(\beta) = \chi_\beta(x).) \end{array} \tag{54}$$

So for $(\alpha, \beta) \in (G^2)^* = G^2 \setminus \{(0_G, 0_G)\}$, we obtain

$$\begin{array}{rcl} \displaystyle\sum_{(x,y)\in G^2} d_{(\alpha,\beta)} f(x, y) & = & \displaystyle\sum_{(x,y)\in G^2} \chi_\alpha(\beta)\chi_\alpha(y) g(\beta + y)\overline{g(y)}\chi_\beta(x) \\ & = & \chi_\alpha(\beta) \displaystyle\sum_{y\in G} \chi_\alpha(y) g(\beta + y)\overline{g(y)} \displaystyle\sum_{x\in G} \chi_\beta(x) \end{array} \tag{55}$$

The sum $\sum_{x\in G}\chi_\beta(x)$ is equal to 0 if $\beta \neq 0_G$ and $|G| \bmod p$ if $\beta = 0_G$ (according to lemma 5.1). Then the right member of the equality (55) is equal to 0 if $\beta \neq 0_G$ and $(|G| \bmod p)\chi_\alpha(\beta)\sum_{y\in G}\chi_\alpha(y)g(\beta+y)\overline{g(y)}$ if $\beta = 0_G$. So when $\beta \neq 0_G$, $\sum_{(x,y)\in G^2} d_{(\alpha,\beta)}f(x,y) = 0$. Now let us assume that $\beta = 0_G$, then because $(\alpha,\beta) \in G^2 \setminus \{(0_G,0_G)\}$, $\alpha \neq 0_G$, we have

$$\begin{aligned}\sum_{(x,y)\in G^2} d_{(\alpha,0_G)}f(x,y) &= (|G| \bmod p)\chi_\alpha(0_G)\sum_{y\in G}\chi_\alpha(y)g(0_G+y)\overline{g(y)} \\ &= (|G| \bmod p)\sum_{y\in G}\chi_\alpha(y) \\ &\quad \text{(because } g \text{ is } \mathcal{S}(\mathrm{GF}(q))\text{-valued)} \\ &= 0 \text{ (because } \alpha \neq 0_G.)\end{aligned} \tag{56}$$

So we have checked that for all $(\alpha,\beta) \in G^2 \setminus \{(0_G,0_G)\}$, $\sum_{(x,y)\in G^2} d_{(\alpha,\beta)}f(x,y) = 0$ and then according to theorem 7.4 this implies that f is bent.

8. Vectorial bent functions over a finite field

In this last section is developed a notion of bentness for $\mathrm{GF}(q)^l$-valued functions defined on G called *vectorial functions* (this is not the same meaning as in the classical literature where it means in general maps from $\mathrm{GF}(2)^m$ to $\mathrm{GF}(2)^n$, see for instance [5]). In order to treat this case in a similar way as in the section 7, we first introduce a special kind of Fourier transform needed to make clear our definitions.

8.1. Multidimensional bent functions

Definition 8.1. Let $f\colon G \to \mathrm{GF}(q)^l$. The multidimensional Fourier transform of f is the map $\widehat{f}^{MD}$ defined as

$$\begin{array}{rccc}\widehat{f}^{MD}: & G & \to & \mathrm{GF}(q)^l \\ & \alpha & \mapsto & \sum_{x\in G}\chi_\alpha(x)f(x)\ .\end{array} \tag{57}$$

If $l = 1$, then it is obvious that the multidimensional Fourier transform coincides with the classical one. Let B the canonical basis of the $\mathrm{GF}(q)$-vector space $\mathrm{GF}(q)^l$ of dimension l, which is orthonormal for the dot-product $\langle\cdot,\cdot\rangle$ (see formula (15)). Let $e \in B$. We define the *coordinate function* f_e of $f\colon G \to \mathrm{GF}(q)^l$ with respect to e as

$$\begin{array}{rccc}f_e: & G & \to & \mathrm{GF}(q) \\ & x & \mapsto & \langle f(x), e\rangle\ .\end{array} \tag{58}$$

Then according to the properties of an orthonormal basis, we observe that

$$f(x) = \sum_{e\in B} f_e(x)e \tag{59}$$

for each $x \in G$. Thanks to coordinate functions, it is possible to give a connection between the Fourier transform from section 6 and its multidimensional counterpart.

Lemma 8.2. *For each $\alpha \in G$, we have*

$$\widehat{f}^{MD}(\alpha) = \sum_{e \in B} \widehat{f}_e(\alpha) e \ . \tag{60}$$

Proof. Let $\alpha \in G$.

$$\begin{aligned} \widehat{f}^{MD}(\alpha) &= \sum_{x \in G} \chi_\alpha(x) f(x) \\ &= \sum_{x \in G} \sum_{e \in B} \chi_\alpha(x) f_e(x) e \\ &= \sum_{e \in B} \left(\sum_{x \in G} f_e(x) \chi_\alpha(x) \right) e \\ &= \sum_{e \in B} \widehat{f}_e(\alpha) e \ . \end{aligned} \tag{61}$$

□

Hereafter in this subsection are established some properties for the multidimensional Fourier transform similar to the corresponding properties of the "one-dimensional" Fourier transform. So let $f : G \to \mathrm{GF}(q)^l$. Let us compute the Fourier transform of $\widehat{f}^{MD}$. Let $\alpha \in G$.

$$\begin{aligned} \widehat{\widehat{f}^{MD}}^{MD}(\alpha) &= \sum_{x \in G} \chi_\alpha(x) \widehat{f}^{MD}(x) \\ &= \sum_{x \in G} \sum_{e \in B} \widehat{f}_e(x) \chi_\alpha(x) e \text{ (according to lemma 8.2)} \\ &= \sum_{E \in B} \left(\sum_{x \in G} \widehat{f}_e(x) \chi_\alpha(x) \right) e \\ &= \sum_{e \in B} \widehat{\widehat{f}}_e(\alpha) e \\ &= (|G| \bmod p) \sum_{e \in B} f_e(-\alpha) e \text{ (according to relation (31))} \\ &= (|G| \bmod p) f(-\alpha) \text{ (according to formula (59))} \ . \end{aligned} \tag{62}$$

The equality $\widehat{\widehat{f}^{MD}}^{MD}(\alpha) = (|G| \bmod p) f(-\alpha)$ will be useful in the sequel. Moreover the following *inversion formula* is proved.

$$\text{For all } \alpha \in G, \ f(\alpha) = (|G| \bmod p)^{-1} \sum_{x \in G} \overline{\chi_x(\alpha)} \widehat{f}^{MD}(x) \ . \tag{63}$$

Now, we present a certain kind of Parseval equation in this context.

Theorem 8.3 (Parseval equation)**.** *Let $f \colon G \to \mathrm{GF}(q)^l$ then*

$$\sum_{x \in G} \mathrm{norm}_l(f(x)) = (|G| \bmod p)^{-1} \sum_{\alpha \in G} \mathrm{norm}_l(\widehat{f}^{MD}(\alpha)) \ . \tag{64}$$

If $f \colon G \to \mathcal{S}(\mathrm{GF}(q)^l)$, then

$$\sum_{\alpha \in G} \mathrm{norm}_l(\widehat{f}^{MD}(\alpha)) = (|G| \bmod p)^2 \ . \tag{65}$$

Proof.

$$\begin{aligned}
\sum_{x\in G}\mathrm{norm}_l(f(x)) &= \sum_{x\in G}\sum_{e\in B}\mathrm{norm}(f_e(x)) \\
&= (|G| \bmod p)^{-1}\sum_{e\in B}\sum_{\alpha\in G}\mathrm{norm}(\widehat{f_e}(\alpha)) \\
&\quad \text{(according to the Parseval equation applied on } f_e) \qquad (66)\\
&= (|G| \bmod p)^{-1}\sum_{\alpha\in G}\sum_{e\in B}\mathrm{norm}(\widehat{f_e}(\alpha)) \\
&= (|G| \bmod p)^{-1}\sum_{\alpha\in G}\mathrm{norm}_l(\widehat{f}^{MD}(\alpha)) \ .
\end{aligned}$$

The second assertion is obvious. □

It is possible, and even more interesting, to obtain this Parseval equation in an alternative way. Let $f, g \in (\mathrm{GF}(q)^l)^G$ and $\alpha \in G$. By replacing the multiplication by the dot-product, we define the *convolutional product* as follows

$$(f * g)(\alpha) = \sum_{x\in G}\langle g(\alpha + x), f(x)\rangle \ . \qquad (67)$$

Since $f * g \colon G \to \mathrm{GF}(q)$, we can compute its one-dimensional Fourier transform

$$\begin{aligned}
\widehat{(f*g)}(\alpha) &= \sum_{x\in G}(f*g)(x)\chi_\alpha(x) \\
&= \sum_{x\in G}\sum_{y\in G}\chi_\alpha(x)\langle g(x+y), f(y)\rangle \\
&= \sum_{x\in G}\sum_{y\in G}\chi_\alpha(x+y)\overline{\chi_\alpha(y)}\langle g(x+y), f(y)\rangle \\
&= \sum_{x\in G}\sum_{y\in G}\langle \chi\alpha(x+y)g(x+y), \chi_\alpha(y)f(y)\rangle \\
&= \sum_{y\in G}\langle\sum_{x\in G}\chi_\alpha(x+y)g(x+y), \chi_\alpha(y)f(y)\rangle \\
&= \sum_{y\in G}\langle \widehat{g}^{MD}(\alpha), \chi_\alpha(y)f(y)\rangle \\
&= \langle \widehat{g}^{MD}(\alpha), \sum_{y\in G}\chi_\alpha(y)f(y)\rangle \\
&= \langle \widehat{g}^{MD}(\alpha), \widehat{f}^{MD}(\alpha)\rangle \ .
\end{aligned} \qquad (68)$$

It is a kind of trivialization of the convolutional product by the Fourier transform. Now let us compute $(f * g)(0_G)$. There are two ways to do this. The first one is given by definition: $(f * g)(0_G) = \sum_{x\in G}\langle g(x), f(x)\rangle$. The second one is given by the inversion formula of the Fourier transform.

$$\begin{aligned}
(f*g)(0_G) &= (|G| \bmod p)^{-1}\sum_{\alpha\in G}\widehat{(f*g)}(\alpha)\overline{\chi_{0_G}(\alpha)} \\
&= (|G| \bmod p)^{-1}\sum_{\alpha\in G}\widehat{(f*g)}(\alpha) \\
&= (|G| \bmod p)^{-1}\sum_{\alpha\in G}\langle \widehat{g}^{MD}(\alpha), \widehat{f}^{MD}(\alpha)\rangle \ .
\end{aligned} \qquad (69)$$

Then we have $\sum_{x\in G}\langle g(x), f(x)\rangle = (|G| \bmod p)^{-1}\sum_{\alpha\in G}\langle \widehat{g}^{MD}(\alpha), \widehat{f}^{MD}(\alpha)\rangle$.
Now let $f = g$, then

$$\sum_{x\in G}\langle f(x), f(x)\rangle = (|G| \bmod p)^{-1}\sum_{\alpha\in G}\langle \widehat{f}(\alpha), \widehat{f}(\alpha)\rangle \tag{70}$$

i.e.,

$$\sum_{x\in G}\mathrm{norm}_l(f(x)) = (|G| \bmod p)^{-1}\sum_{\alpha\in G}\mathrm{norm}_l(\widehat{f}(\alpha)) \ . \tag{71}$$

8.2. Multidimensional bent functions

In the paper [17] is introduced the notion of multidimensional bentness for $\mathcal{H}$-valued functions defined on a finite Abelian group G, where $\mathcal{H}$ is a finite-dimensional Hermitian space. In this subsection, we translate this notion in our special kind of Hermitian structure.

Definition 8.4. Let $f : G \to \mathcal{S}(\mathrm{GF}(q)^l)$. The function f is said *multidimensional bent* if for all $\alpha \in G$, $\mathrm{norm}_l(\widehat{f}^{MD}(\alpha)) = (|G| \bmod p)$.

Lemma 8.5. *Let $f\colon G \to \mathrm{GF}(q)^l$. Then, $f(x) = (\underbrace{0,\ldots,0}_{l \text{ times}})$ for all $x \in G^*$ if, and only if, $\widehat{f}^{MD}(\alpha) = f(0_G)$ for all $\alpha \in G$.*

Proof. $\Rightarrow$) $\widehat{f}^{MD}(\alpha) = \sum_{x\in G}\chi_\alpha(x)f(x) = f(0_G)\ \forall\alpha \in G$.
$\Leftarrow$) $f(x) = (|G| \bmod p)^{-1}\sum_{\alpha\in G}\overline{\chi_\alpha(x)}\widehat{f}^{MD}(\alpha)$ (by the inversion formula of the multidimensional Fourier transform). Then by assumption,

$$f(x) = (|G| \bmod p)^{-1}f(0_G)\sum_{\alpha\in G}\chi_\alpha(x) = (\underbrace{0,\ldots,0}_{l \text{ times}})$$

if $x \in G^*$, and $f(0_G)$ otherwise. □

This technical result holds in particular when $l = 1$ which is lemma 7.2.

As in the one-dimensional setting, there exists a combinatorial characterization of the multidimensional bentness. We define a kind of derivative for $\mathrm{GF}(q)^l$-valued functions. Another time we use the natural "multiplication" of $\mathrm{GF}(q)^l$ which is its dot-product.

Definition 8.6. Let $f\colon G \to \mathrm{GF}(q)^l$ and $\alpha \in G$. The *derivative of f in direction α* is defined by

$$\begin{array}{rccl} d_\alpha f\colon & G & \to & \mathrm{GF}(q) \\ & x & \mapsto & \langle f(\alpha + x), f(x)\rangle \ . \end{array} \tag{72}$$

This derivative measures the default of orthogonality between $f(x)$ and $f(\alpha+x)$.

Proposition 9. *Let $f\colon G \to \mathcal{S}(\mathrm{GF}(q)^l)$. Then, f is bent if, and only if, for all $\alpha \in G^*$, $\widehat{d_\alpha f}(0_G) = 0$.*

Proof. Let us define the following autocorrelation function

$$\begin{array}{rccc} AC_f: & G & \to & \mathrm{GF}(q) \\ & \alpha & \mapsto & \widehat{d_\alpha f}(0_G)\ . \end{array} \tag{73}$$

We have

$$\begin{array}{rcl} \widehat{d_\alpha f}(0_G) & = & \displaystyle\sum_{x\in G} d_\alpha f(x)\chi_{0_G}(x) \\ & = & \displaystyle\sum_{x\in G} d_\alpha f(x) \\ & = & \displaystyle\sum_{x\in G} \langle f(\alpha+x), f(x)\rangle \\ & = & (f*f)(\alpha)\ . \end{array} \tag{74}$$

Let us compute $\widehat{AC_f}(\alpha)$.

$$\begin{array}{rcl} \widehat{AC_f}(\alpha) & = & \displaystyle\sum_{x\in G} AC_f(x)\chi_\alpha(x) \\ & = & \displaystyle\sum_{x\in G} (f*f)(x)\chi_\alpha(x) \\ & = & \widehat{(f*f)}(\alpha) \\ & = & \langle \widehat{f}^{MD}(\alpha), \widehat{f}^{MD}(\alpha)\rangle \text{ (by the formula (68))} \\ & = & \mathrm{norm}_l(\widehat{f}^{MD}(\alpha))\ . \end{array} \tag{75}$$

Then we have
$\forall \alpha \in G^*,\ \widehat{d_\alpha f}(0_G) = 0$
$\Leftrightarrow \forall \alpha \in G^*,\ AC_f(\alpha) = 0$
$\Leftrightarrow \forall \alpha \in G,\ \widehat{AC_f}(\alpha) = AC_f(0_G)$ (according to lemma 8.5)
$\Leftrightarrow \forall \alpha \in G,\ \mathrm{norm}_l(\widehat{f}^{MD}(\alpha)) = AC_f(0_G)$.
As $AC_f(0_G) = (f*f)(0_G) = \displaystyle\sum_{x\in G}\langle f(x), f(x)\rangle = \sum_{x\in G}\mathrm{norm}(f(x)) = (|G| \bmod p)$ (since f is $\mathcal{S}(\mathrm{GF}(q)^l)$-valued), we conclude with the expected result. □

References

[1] A.S. Ambrosimov, *Properties of bent functions of q-valued logic over finite fields*, Discrete Mathematics and Applications **4**(4) (1994), 341–350.

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

[3] R. E. Blahut, "Theory and practice of error control codes," Addison-Wesley, 1983.

[4] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM Journal of Computing **32**(3) (2003), 586–615.

[5] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes," Chapter 9 of Boolean Models and Methods in Mathematics, Computer Science, and Engineering (eds. Yves Crama and Peter L. Hammer), Encyclopedia of Mathematics and its Applications **134** (2010), 398–469.

[6] C. Carlet and C. Ding, *Highly nonlinear mappings*, Journal of Complexity **20**(2–3) (2004), 205–244.

[7] C. Carlet and S. Dubuc, *On generalized bent and q-ary perfect nonlinear functions*, in "Proc. of the Fifth International Conference on Finite Fields and Applications F_q5" (eds. D. Jugnickel and H. Niederreiter), (2001), 81–94

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

[9] H. Dobbertin, G.Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit, *Construction of Bent Functions via Niho Power Functions*, Journal of Combinatorial Theory, Serie A **113** (2006), 779–798.

[10] E. Hewitt and K.A. Ross, "Abstract Harmonic Analysis, vol 1 (2nd edition)," volume 115 of Comprehensive Studies in Mathematics, Springer, 1994.

[11] P.V. Kumar, R.A. Scholtz and L.R. Welch, *Generalized bent functions and their properties*, Journal of Combinatorial Theory A **40** (1985), 99–107.

[12] 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.

[13] M. Matsui, *Linear cryptanalysis for DES cipher*, in "Proc. Advances in cryptology - Eurocrypt'93" (ed. Tor Hellesth), Lecture Notes in Computer Science **765**, Springer, (1994), 386–397.

[14] R. L. McFarland, *A family of difference sets in non-cyclic groups*, Journal of Combinatorial Theory **15** (1973), 1–10.

[15] S. McLane, "Categories for the working mathematician (2nd edition)," volume 5 of Graduate Texts in Mathematics, Springer, 1998.

[16] K. Nyberg, *Constructions of bent functions and difference sets*, in "Proc. Advances in cryptology - Eurocrypt'90" (ed. Ivan Damgård), Lecture Notes in Computer Science **473**, Springer, (1990), 151–160.

[17] L. Poinsot, *Multidimensional bent functions*, GESTS International Transactions on Computer Science and Engineering **18**(1) (2005), 185–195.

[18] O. S. Rothaus, *On bent functions*, Journal of Combinatorial Theory A **20** (1976), 300–365.