Harmonic Analysis and A Bentness-Like Notion in Certain Finite Abelian Groups over Some Finite Fields

[1]Laurent Poinsot and [2*]Nadia El Mrabet
[1] *University Paris 13, Sorbonne Paris Cité, LIPN, CNRS (UMR 7030), France,*
[2] *University Paris 8, LIASD, France*
Email: [1] *laurent.poinsot@lipn.univ-paris13.fr,* [2]*elmrabet@ai.univ-paris8.fr*
Website: [1] *http://lipn.univ-paris13.fr/poinsot/,* [2]*http://www.ai.univ-paris8.fr/elmrabet/*

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

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

1. INTRODUCTION

The most simple Hermitian structure is obtained from the degree two field extension of the complex numbers over the real numbers. It has many applications and in particular provides the usual theory of characters for finite Abelian groups and the existence of an associated Fourier transform. 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 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 cyclic groups whose order 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. As an illustration of our theory of modular characters one introduces and studies the corresponding cryptographic notion of bent functions in this 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. As usual $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$.

The *characters* are 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 $\hat{G}$ and called the *dual group of* G. A classical result claims that G and its dual are isomorphic (essentially because $\mathcal{S}(\mathbb{C})$ contains an isomorphic copy of all cyclic groups). The image in $\hat{G}$ 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),

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

Definition 1. Let G be a finite Abelian group and $f: G \to \mathbb{C}$. The Fourier transform of f is defined as

$$\begin{array}{rccl} \hat{f}: & G & \to & \mathbb{C} \\ & \alpha & \mapsto & \sum_{x\in G} f(x)\chi_\alpha(x) \ . \end{array} \tag{4}$$

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

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

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, and $*$ is the convolution product defined by

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

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

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

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

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

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

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

3. HERMITIAN STRUCTURE OVER FINITE FIELDS

In this section we recall some results about an Hermitian structure in some kinds of finite fields. This section is directly inspired from (Dobbertin, et al., 2006) of which we follow the notations, and is 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 usual $\mathrm{GF}(q)$ 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 $\mathrm{GF}(q)$

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

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 2. *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*

$$\overline{x_1 + x_2} = \overline{x_1} + \overline{x_2}, \qquad \overline{-x_1} = -\overline{x_1}, \overline{x_1 x_2} = \overline{x_1}\ \overline{x_2}, \qquad \overline{\overline{x_1}} = x_1$$

Proof. The three first equalities 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

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

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.

4. CHARACTERS 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. 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 have orders that divide $\sqrt{q}+1$.

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

Definiton 3. (*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 $\hat{G}$ the set of all characters of G that we call its *dual*. When equipped with the point-wise multiplication, $\hat{G}$ is a finite Abelian group. One recall that this multiplication is defined as

$$\forall \chi, \chi' \in \hat{G},\ \chi\chi' : x \mapsto \chi(x)\chi'(x). \tag{15}$$

As already mentioned 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 $\{0, \dots, d-1\}$ of $\mathbb{Z}$.

Theorem 1. *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 $j \in \mathbb{Z}_d$,

$$\chi_j : \begin{cases} \mathbb{Z}_d & \to & \mathcal{S}_d(\mathrm{GF}(q)) \\ k & \mapsto & (u_d^j)^k = u_d^{jk}. \end{cases} \tag{16}$$

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 $k \in \{0, \dots, d-1\}$, which gives

$$\chi(k) = u_d^{jk}. \tag{17}$$

In this equality, we have denoted $\chi(1)$ by u_d^j for $j \in \{0, \dots, d-1\}$ since $\chi(1)$ is a d-th root of the unity in $\mathcal{S}(\mathrm{GF}(q))$. Then the character χ belongs to $\{\chi_0, \dots, \chi_{d-1}\}$. Conversely, we observe that for $j \in \{1, \dots, d-1\}$, 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.

$$\begin{array}{rccc} \Psi: & \mathbb{Z}_d & \to & \widehat{\mathbb{Z}_d} \\ & j & \mapsto & \chi_j \ . \end{array} \tag{18}$$

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 $\mathbb{Z}_d$.

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

$$\Phi: \begin{cases} (\widehat{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}}) & \to \quad \widehat{\mathbb{Z}_{d_1}} \times \widehat{\mathbb{Z}_{d_2}} \\ \chi & \mapsto \quad (\chi \circ i_1, \chi \circ i_2) \end{cases} \tag{19}$$

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

$$x \cdot y = \sum_{i=1}^{m} x_i y_i \in \mathbb{Z}_d \tag{20}$$

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

$$\begin{array}{rccc} \chi_\alpha: & \mathbb{Z}_d^m & \to & \mathcal{S}_d(\mathrm{GF}(q)) \\ & x & \mapsto & u_d^{\alpha \cdot x} \end{array} \tag{21}$$

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* $\hat{G}$ *are isomorphic.*

If $G = \prod_{i=1}^{N} \mathbb{Z}_{d_i}^{m_i}$ satisfies the assumption of the corollary 1, then for $\alpha = (\alpha_1, \dots, \alpha_N) \in G$ one has

$$\chi_\alpha: G \quad \to \mathcal{S}(\mathrm{GF}(q))$$

$$x = (x_1, \dots, x_N) \quad \mapsto \prod_{i=1}^{N} u_{d_i}^{\alpha_i \cdot x_i} \tag{22}$$

where for each $i \in \{1, \dots, N\}$, 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 $i \in \{1, \dots, N\}$, d_i divides $\sqrt{q}+1$, so that we have at our disposal a specific isomorphism given by the formula (22) between G and $\hat{G}$.*

The dual $\hat{G}$ of G is constructed and is shown to be isomorphic to G. We may also be interested into the bidual $\hat{\hat{G}}$ of G, namely the dual of $\hat{G}$. Similarly to the usual situation of complex-valued characters, we prove that G and its bidual are canonically isomorphic. It is already clear that $G \cong \hat{\hat{G}}$ (because $G \cong \hat{G}$ and $\hat{G} \cong \hat{\hat{G}}$). But this isomorphism is far from being canonical since it depends on a decomposition of G, and of $\hat{G}$, and choices for generators of each cyclic factor in the given decomposition. We observe that the map $e: G \to \hat{\hat{G}}$ defined by $e(x)(\chi) = \chi(x)$ for every $x \in G, \chi \in \hat{G}$ is a group homomorphism. To prove that it is an isomorphism it suffices to check that e is one-to-one (since G and $\hat{\hat{G}}$ have the same order). Let $x \in \ker(e)$. Then, for all $\chi \in \hat{G}, \chi(x) = 1$. Let us fix an isomorphism $\alpha \in G \to \chi_\alpha \in \hat{G}$ as in the formula (22). 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 (Hewitt & Ross, 1994)). 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 $Ab_{\sqrt{q}+1}$ 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 $Ab_{\sqrt{q}+1}$, then $G \cong \hat{G}$. Moreover, $\widehat{(\cdot)}$ defines a contravariant functor (see (McLane, 1998)) from $Ab_{\sqrt{q}+1}$ to itself. Indeed, if $\phi: G \to H$ is a homomorphism of groups (where G, H belongs to $Ab_{\sqrt{q}+1}$), then $\hat{\phi}: \hat{H} \to \hat{G}$ defined by $\hat{\phi}(\chi) = \chi \circ \phi$ is a homomorphism of groups. Then, we have the following duality theorem.

Theorem 2 (Duality). *The covariant (endo-)functor $\widehat{\widehat{(\cdot)}}: Ab_{\sqrt{q}+1} \to Ab_{\sqrt{q}+1}$ is a (functorial) isomorphism (this means in particular that $G \cong \hat{\hat{G}}$).*

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 $kx = x \underbrace{+ \cdots +}_{k \text{ times}} x$ 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 explicit the identification of $\mathrm{GF}(p)$ and $\mathbb{Z}_p$.

Lemma 1. *Let G be a finite Abelian group. For $\chi \in \hat{G}$,*

$$\sum_{x \in G} \chi(x) = \begin{cases} 0 & \text{if } \chi \neq 1 \ , \\ (|G| \bmod p) & \text{if } \chi = 1 \ . \end{cases} \tag{23}$$

Proof. If $\chi = 1$, then $\sum_{x \in G} 1 = (|G| \bmod p)$ 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

$$\chi(x_0) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(x_0 + x) = \sum_{y \in G} \chi(y), \tag{24}$$

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

Definition 4. *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*

$$\langle f, g \rangle = \sum_{x \in G} f(x) \overline{g(x)} \in \mathrm{GF}(q). \tag{25}$$

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 $f : \mathbb{Z}_2 \to \mathrm{GF}(2^{2n})$ 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. Let G be a finite Abelian group. For all $(\chi_1, \chi_2) \in \hat{G}^2$ then the orthogonality relations holds

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2, \\ |G| \bmod p & \text{if } \chi_1 = \chi_2. \end{cases} \tag{26}$$

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

$$\langle \chi_1, \chi_2 \rangle = \sum_{x \in G} \chi(x). \tag{27}$$

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 1.

Remark 1. The term *orthogonality* would be abusive if $|G| \bmod p = 0$, because then $\sum_{x \in G} \chi(x) = 0$ for all $\chi \in \hat{G}$. Nevertheless from the assumption 3 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

There is already a Fourier transform with values in some finite field called *Mattson-Solomon transform* (Blahut, 1983) but it is not useful in our setting. 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.

$$\begin{array}{rccl} \hat{f}: & \hat{G} & \to & \mathrm{GF}(q) \\ & \chi & \mapsto & \sum_{x \in G} f(x) \chi(x) \ . \end{array} \tag{28}$$

Since $G = \prod_{i=1}^{N} \mathbb{Z}_{d_i}^{m_i}$, we define, by the isomorphism between G and its dual,

$$\begin{aligned} \hat{f}: \quad G &\to \mathrm{GF}(q) \\ \alpha &\mapsto \sum_{x\in G} f(x)\chi_\alpha(x) = \sum_{x\in G} f(x) \prod_{i=1}^{N} u^{\frac{(\sqrt{q}+1)\alpha_i \cdot x_i}{d_i}} \end{aligned} \tag{29}$$

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

$$\begin{aligned} \hat{\hat{f}}(\alpha) &= \sum_{x\in G} \hat{f}(x)\chi_\alpha(x) \\ &= \sum_{x\in G} \sum_{y\in G} f(y)\chi_x(y)\chi_\alpha(x) \\ &= \sum_{x\in G} \sum_{y\in G} f(y)\chi_y(x)\chi_\alpha(x) \\ &= \sum_{y\in G} f(y) \sum_{x\in G} \chi_{\alpha+y}(x) \\ &= (|G| \bmod p) f(-\alpha) \end{aligned} \tag{30}$$

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 $f \mapsto \hat{f}$ 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 $\hat{f} \in \mathrm{GF}(q)^G$ 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 $x \in G$,

$$f(x) = (|G| \bmod p)^{-1} \sum_{\alpha\in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)} \tag{31}$$

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

$$(f * g)(\alpha) = \sum_{x\in G} f(x)g(-x+\alpha). \tag{32}$$

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

$$\widehat{(f * g)}(\alpha) = \hat{f}(\alpha)\hat{g}(\alpha) \ . \tag{33}$$

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

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

$$\begin{aligned} &= \sum_{x\in G}\sum_{y\in G} f(y)g(-y+x)\chi_\alpha(y-y+x) \\ &= \sum_{x\in G}\sum_{y\in G} f(y)g(-y+x)\chi_\alpha(y)\chi_\alpha(-y+x) \\ &= \hat{f}(\alpha)\hat{g}(\alpha). \end{aligned} \tag{34}$$

The group-algebra $\mathrm{GF}(q)[G]$ of G over $\mathrm{GF}(q)$ is the $\mathrm{GF}(q)$-vector space $\mathrm{GF}(q)^G$ equipped with convolution. The Fourier transform $\widehat{(\cdot)}$ is an algebra isomorphism from the group-algebra $\mathrm{GF}(q)[G]$ 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). It is easy to see that $\hat{\delta}_x = \chi_x$. 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 $\hat{f}$ of $f \in \mathrm{GF}(q)^G$ is the decomposition of f into the basis of characters (even if a family of elements of $\mathrm{GF}(q)^G$ is orthogonal with respect to the inner-product $\langle\cdot,\cdot\rangle$ of $\mathrm{GF}(q)^G$ this does not ensure linear independence because $\langle\cdot,\cdot\rangle$ is not positive-definite).

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

$$\sum_{x\in G} f(x)\overline{g(x)} = (|G| \bmod p)^{-1} \sum_{\alpha\in G} \hat{f}(\alpha)\overline{\hat{g}(\alpha)}. \tag{35}$$

Proof. Let us define the following functions with $h: G \to \mathrm{GF}(q)$,

$$\begin{aligned} I_G:\ & G \to G \\ & x \mapsto -x \\ & \text{and} \\ \overline{h}:\ & G \to \mathrm{GF}(q) \\ & x \mapsto \overline{h(x)}\ . \end{aligned} \tag{36}$$

Then $(f * \overline{g} \circ I_G)(0_G) = \sum_{x\in G} f(x)\overline{g(x)}$. By the inversion formula:

$$\begin{aligned} (f * \overline{g} \circ I_G)(0_G) &= (|G| \bmod p)^{-1} \textstyle\sum_{\alpha\in G} \widehat{(f * \overline{g} \circ I_G)}(\alpha) \\ &= (|G| \bmod p)^{-1} \textstyle\sum_{\alpha\in G} \hat{f}(\alpha)\widehat{(\overline{g} \circ I_G)}(\alpha). \end{aligned} \tag{37}$$

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

$$\begin{aligned} \widehat{(\overline{g} \circ I_G)}(\alpha) &= \sum_{x\in G} (\overline{g} \circ I_G)(x)\chi_\alpha(x) \\ &= \sum_{x\in G} \overline{g(-x)}\chi_\alpha(x) \\ &= \sum_{x\in G} \overline{g(x)}\chi_\alpha(-x) \\ &= \sum_{x\in G} \overline{g(x)}(\chi_\alpha(x))^{-1} \\ &= \sum_{x\in G} \overline{g(x)\chi_\alpha(x)} \\ &= \overline{\sum_{x\in G} g(x)\chi_\alpha(x)} \\ &= \hat{g}(\alpha) \end{aligned} \tag{38}$$

Then we obtain the equality that ensures the correct result

$$(f * \overline{g} \circ I_G) = (|G| \bmod p)^{-1} \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\hat{g}(\alpha)} \tag{39}$$

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

$$\sum_{x \in G} \mathrm{norm}(f(x)) = (|G| \bmod p)^{-1} \sum_{\alpha \in G} \mathrm{norm}(\hat{f}(\alpha)) \ . \tag{40}$$

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

$$\sum_{\alpha \in G} \mathrm{norm}(\hat{f}(\alpha)) = (|G| \bmod p)^2 \tag{41}$$

7. BENT FUNCTIONS OVER A FINITE FIELD

In the traditional setting, i.e., for complex-valued functions defined on any finite Abelian group G, bent functions ((Carlet and Ding, 2004), (Dillon, 1974), (Logachev, Salnikov, and Yashchenko, 1997), (Nyberg, 1990) (Rothaus, 1976)) are those maps $f: G \to \mathcal{S}(\mathbb{C})$ such that for each $\alpha \in G$,

$$|\hat{f}(\alpha)|^2 = |G| \ . \tag{42}$$

This notion is closely related to some famous cryptanalysis namely the differential (Biham and Shamir, 1991) and linear (Matsui, 1994) attacks on secret-key cryptosystems. We translate this concept in the current finite-field setting as follows.

Definition 6. *The map* $f: G \to \mathcal{S}(\mathrm{GF}(q))$ *is called bent if for all* $\alpha \in G$,

$$\mathrm{norm}(\hat{f}(\alpha)) = (|G| \bmod p). \tag{43}$$

7.1 Derivative and bentness

Propositon 7. (Logachev, Salnikov, and Yashchenko, 1997) *Let* $f: G \to \mathcal{S}(\mathbb{C})$. *The function* f *is bent if, and only if, for all* $\alpha \in G^*$,

$$\sum_{x \in G} f(\alpha + x)\overline{f(x)} = 0. \tag{44}$$

Now let $f: G \to \mathrm{GF}(q)$. For each $\alpha \in G$, we define the derivative of f in direction α as

$$\begin{array}{rccl} d_\alpha f: & G & \to & \mathrm{GF}(q) \\ & x & \mapsto & f(\alpha + x)\overline{f(x)} \ . \end{array} \tag{45}$$

Lemma 2. *Let* $f: G \to \mathrm{GF}(q)$. *We have*

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

Proof.

1. $\Rightarrow \hat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x) = f(0_G)\chi_\alpha(0_G) = f(0_G)$,
   $\Leftarrow$ According to the inversion formula,

$$\begin{aligned} f(x) &= (|G| \bmod p)^{-1} \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)} \\ &= f(0_G)(|G| \bmod p)^{-1} \sum_{\alpha \in G} \chi_{-x}(\alpha) \\ &= 0 \quad \text{for all} \quad x \neq 0_G \ . \end{aligned} \tag{46}$$

2. $\Rightarrow f(x) = (|G| \bmod p)^{-1} \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)} = \hat{f}(0_G)(|G| \bmod p)^{-1}, \Leftarrow \hat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x) = \text{constant} \sum_{x \in G} \chi_\alpha(x) = 0$ for all $\neq 0_G$.

Lemma 3. Let $f: G \to GF(q)$. We define the autocorrelation function of f as

$$\begin{aligned} AC_f: \quad G &\to \mathrm{GF}(q) \\ \alpha &\mapsto \sum_{x \in G} d_\alpha f(x) \ . \end{aligned} \tag{47}$$

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

$$\begin{aligned} \widehat{AC_f}(\alpha) &= \sum_{x \in G} AC_f(x)\chi_\alpha(x) \\ &= \sum_{x \in G} \sum_{y \in G} d_x f(y)\chi_\alpha(x) \\ &= \sum_{x \in G} \sum_{y \in G} f(xy)\overline{f(y)}\chi_\alpha(xy)\overline{\chi_\alpha(y)} \\ &= \hat{f}(\alpha)\overline{\hat{f}(\alpha)} \\ &= \mathrm{norm}(\hat{f}(\alpha)) \ . \end{aligned} \tag{48}$$

Theorem 3. *The function $f: G \to \mathcal{S}(\mathrm{GF}(q))$ is bent if, and only if, for all $\alpha \in G^*$, $\sum_{x \in G} d_\alpha f(x) = 0$.*
Proof. $\forall \alpha \in G^*, \ \sum_{x \in G} d_\alpha f(x) = 0$
$\Leftrightarrow \forall \alpha \in G^*, \ AC_f(\alpha) = 0$
$\Leftrightarrow \forall \alpha \in G, \ \widehat{AC_f}(\alpha) = AC_f(0_G)$
(according to lemma 2)
$\Leftrightarrow \forall \alpha \in G, \ \mathrm{norm}(\hat{f}(\alpha)) = \sum_{x \in G} f(x)\overline{f(x)}$
(according to lemma 3)
$\Leftrightarrow \forall \alpha \in G, \ \mathrm{norm}(\hat{f}(\alpha)) = \sum_{x \in G} \mathrm{norm}(f(x))$
$\Leftrightarrow \forall \alpha \in G, \ \mathrm{norm}(\hat{f}(\alpha)) = (|G| \bmod p)$
(because f is $\mathcal{S}(\mathrm{GF}(q))$-valued.)

7.2 Dual bent function

Again by analogy to the traditional notion (Carlet and Dubuc, 2001; Kumar, Scholtz, and Welch, 1985), 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 *law of quadratic reciprocity*, we can add the following requirement (only needed for proposition 8).

Assumption 4. *If the prime number p is ≥ 3, then $|G|$ must also satisfy $|G|^{\frac{p-1}{2}} \equiv 1 (\bmod p)$. 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

$$\begin{aligned}((|G| \bmod p)^{\frac{p+1}{4}})^2 &= (|G| \bmod p)^{\frac{p+1}{2}} \\ &= (|G| (\bmod p))(|G| (\bmod p))^{\frac{p-1}{2}} \\ &= |G| (\bmod p).\end{aligned}$$

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

$$\begin{array}{rccl} \tilde{f}: & G & \to & \mathcal{S}(\mathrm{GF}(q)) \\ & \alpha & \mapsto & (|G| \bmod p)^{-\frac{1}{2}} \hat{f}(\alpha) \ . \end{array} \tag{49}$$

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

$$\begin{aligned} \tilde{f}(\alpha)\overline{\tilde{f}(\alpha)} &= (|G| \bmod p)^{-\frac{1}{2}} \hat{f}(\alpha) (|G| \bmod p)^{-\frac{1}{2}} \overline{\hat{f}(\alpha)} \\ &= (|G| \bmod p)^{-1} \mathrm{norm}(\hat{f}(\alpha)) \\ &= 1 \ \ (\text{since } f \text{ is bent.}) \end{aligned} \tag{50}$$

Let us check that the bentness property holds for $\tilde{f}$. Let $\alpha \in G$. We have $\hat{\tilde{f}}(\alpha) = (|G| \bmod p)^{-\frac{1}{2}} (|G| \bmod p) f(-\alpha)$ (by (30)). Then

$$\begin{aligned} \hat{\tilde{f}}(\alpha)\overline{\hat{\tilde{f}}(\alpha)} &= (|G| \bmod p) f(-\alpha) \overline{f(-\alpha)} \\ &= (|G| \bmod p) \mathrm{norm}\big(f(-\alpha)\big) \\ &= (|G| \bmod p) \big(\text{since } f \text{ is } \mathcal{S}\big(\mathrm{GF}(q)\big) - \text{valued.}\big) \end{aligned} \tag{51}$$

7.3 Construction of bent functions

We present a simple version of the well-known Maiorana-McFarland construction ((Dillon, 1974), (McFarland, 1973)) for our bent functions.
Let $g: G \to \mathcal{S}(\mathrm{GF}(q))$ be any function. Let f be the following function.

$$\begin{array}{rccl} f: & G^2 & \to & \mathcal{S}(\mathrm{GF}(q)) \\ & (x, y) & \mapsto & \chi_x(y) g(y) \ . \end{array} \tag{52}$$

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 3. Let $\alpha, \beta, x, y \in G$.

$$\begin{aligned} d_{(\alpha,\beta)}f(x,y) &= f(\alpha+x,\beta+y)\overline{f(x,y)} \\ &= \chi_{\alpha+x}(\beta+y)g(\beta+y)\overline{\chi_x(y)}\ \overline{g(y)} \\ &= \chi_\alpha(\beta+y)\chi_x(\beta+y)g(\beta+y)\overline{\chi_x(y)}\ \overline{g(y)} \\ &= \chi_\alpha(\beta)\chi_\alpha(y)\chi_x(\beta)\chi_x(y)g(\beta+y)\overline{\chi_x(y)}\ \overline{g(y)} \\ &= \chi_\alpha(\beta)\chi_\alpha(y)g(\beta+y)\overline{g(y)}\chi_x(\beta) \\ &= \chi_\alpha(\beta)\chi_\alpha(y)g(\beta+y)\overline{g(y)}\chi_\beta(x) \end{aligned} \tag{53}$$

because $\chi_x(\beta) = \chi_\beta(x)$.
So for $(\alpha,\beta) \in (G^2)^* = G^2\backslash\{(0_G,0_G)\}$, we obtain

$$\begin{aligned} \sum_{(x,y)\in G^2} d_{(\alpha,\beta)}f(x,y) &= \sum_{(x,y)\in G^2} \chi_\alpha(\beta)\chi_\alpha(y)g(\beta+y)\overline{g(y)}\chi_\beta(x) \\ &= \chi_\alpha(\beta)\sum_{y\in G}\chi_\alpha(y)g(\beta+y)\overline{g(y)}\sum_{x\in G}\chi_\beta(x) \end{aligned} \tag{54}$$

The sum $\sum_{x\in G}\chi_\beta(x)$ is equal to 0 if $\beta \neq 0_G$ and $|G|\text{mod p}$ if $\beta = 0_G$ (according to lemma 1). Then the right member of the equality (54) is equal to 0 if $\beta \neq 0_G$ and $(|G|\text{mod p})\chi_\alpha(\beta)\sum_{y\in G}\chi_\alpha(y)g(\beta+y)\overline{g(y)}$ 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 $(\alpha,\beta) \in G^2\backslash\{(0_G,0_G)\}$, $\alpha \neq 0_G$, we have

$$\begin{aligned} \sum_{(x,y)\in G^2} d_{(\alpha,0_G)}f(x,y) &= (|G|\text{mod p})\chi_\alpha(0_G)\sum_{y\in G}\chi_\alpha(y)g(0_G+y)\overline{g(y)} \\ &= (|G|\text{mod p})\sum_{y\in G}\chi_\alpha(y) \\ &\quad \text{(because } g \text{ is } \mathcal{S}(\mathrm{GF}(q)) - \text{valued)} \\ &= 0 \quad \text{(because } \alpha = 0_G.) \end{aligned} \tag{55}$$

So we have checked that for all $(\alpha,\beta) \in G^2\backslash\{(0_G,0_G)\}$ $\sum_{(x,y)\in G^2} d_{(\alpha,\beta)}f(x,y) = 0$ and then according to theorem 3 this implies that f is bent.

8. CONCLUSION AND PERSPECTIVES

There is a close analogy between any quadratic extension of a finite field and the extension of the complex numbers over the field of real numbers. Indeed in both cases it is possible to define an Hermitian structure on the field extension based on a conjugation operation. As in the usual case this structure makes it possible to an introduce a notion of finite field valued characters of (some) finite Abelian groups. These characters form a basis (orthogonal in a certain sense) of the algebra of the group over the base finite field. With this characters in hand it is then possible to introduce a Fourier transform that shares the same properties as the usual one. The study of the Hermitian structure on a quadratic extension and of its consequences was the main objective of this contribution. Because the cryptographic notion of bent functions (particular highly non linear functions) is directly based on the Fourier transform it makes sense also to study this kind of functions in this new setting. This was the second objective of this contribution, achieved by providing two constructions of (finite field valued) bent functions. As an immediate perspective of our work is the analysis of the connections between the usual notion of bent functions and that introduced in the contribution. The relations between the two kinds of bent functions, if any, were outside the scope of this paper but should be the main goal of our future researches on this subject.

9. ACKNOWLEDGMENT

One the authors, Nadia El Mrabet, wishes to acknowledge support from Agence Nationale de la Recherche (France) under project ANR INS 2012 SYMPATIC.

REFERENCES

Ambrosimov, A. S. 1994. Properties of bent functions of q-valued logic over. *Discrete Mathematics and, 4*(4), 341-350.

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

Blahut, R. E. 1983. *Theory and practice of error control codes.* Addison-Wesley.

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

Carlet, C. 2010. Boolean Functions for Cryptography and Error Correcting Codes. In Y. Crama, and P. L. Hammer (Eds.), *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (pp. 398-469). New York: Cambridge University Press.

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

Carlet, C., and Dubuc, S. 2001. On generalized bent and q-ary perfect nonlinear functions. In D. Jugnickel, and H. Niederreiter (Ed.), *Fifth International Conference on Finite Fields and Applications Fq5*, (pp. 81-94).

Dillon, J. F. 1974. *Elementary Hadamard difference sets (Ph.D Thesis).* University of Maryland.

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

Hewitt, E., and Ross, K. A. 1994. *Abstract Harmonic Analysis* (2 ed., Vol. 1). Springer.

Kumar, P. V., Scholtz, R. A., and Welch, L. R. 1985. Generalized bent functions and their properties. *Journal of Combinatorial Theory A, 40*, 99-107.

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

Matsui, M. 1994. Linear cryptanalysis for DES cipher. In T. Hellesth (Ed.), *Advances in cryptology - Eurocrypt'93* (pp. 386-397). Springer.

McFarland, R. L. 1973. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory, 15*, 1-10.

McLane, S. 1998. *Categories for the working mathematician* (2nd ed., Vol. 5). Springer.

Nyberg, K. 1990. Constructions of bent functions and difference sets. In I. Damgard (Ed.), *Advances in cryptology - Eurocrypt'90*, (pp. 151-160).

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

Rothaus, O. S. 1976. On bent functions. *Journal of Combinatorial Theory A, 20*, 300-365.