



A new characterization of group action-based perfect nonlinearity

Laurent Poinso

► To cite this version:

Laurent Poinso. A new characterization of group action-based perfect nonlinearity. Discrete Applied Mathematics, 2009, 157 (8), pp.1848-1857. <10.1016/j.dam.2009.02.001>. <hal-00460343>

HAL Id: hal-00460343

<https://hal.science/hal-00460343v1>

Submitted on 20 Dec 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

A new characterization of group action-based perfect nonlinearity

Laurent Poinot

Laboratoire d'Informatique Paris-Nord 13 - UMR CNRS 7030

Institut Galile

Universit Paris-Nord 13

Avenue J. B. Clment

93430 Villetaneuse

France

laurent.poinot@lipn.univ-paris13.fr

Abstract

The left-regular multiplication is explicitly embedded in the notion of perfect nonlinearity. But it exists many other group actions and by replacing translations by another group action has been recently introduced the new concept of group actions based perfect nonlinearity. In this paper we show that this generalized concept of nonlinearity is actually equivalent to a new bentness notion that deals with functions defined on a finite abelian group G that acts on a finite set X and with values in the finite-dimensional vector space of complex-valued functions defined on X .

Key words:

Bent functions, perfect nonlinearity, finite abelian groups, group actions, G -perfect nonlinearity, finite-dimensional hermitian spaces

1 Introduction

The DES cryptosystem is vulnerable to a differential attack (1) unless the system is designed so the difference of outputs from the S-boxes is “balanced” by using a perfect nonlinear function (11). This well-known cryptographic concept hides the assumption that the internal operation considered is the modulo-2 sum. But there are many other possible choices to operate on bit strings, other group actions on the abelian 2-group \mathbb{Z}_2^m . Then the notion of perfect nonlinearity can naturally be extended by using other group actions. Actually if we consider two finite abelian groups G and H such that G acts on a finite nonempty set X , a function $f : X \rightarrow H$ is said G -perfect nonlinear

(6; 7) if for all nonzero $\alpha \in G$ the “difference” $x \mapsto f(\alpha.x) - f(x)$, where $\alpha.x$ is the action of α on $x \in X$, is balanced, or in other words, its values are equidistributed over H . So this is exactly the notion of perfect nonlinearity in the finite abelian groups setting where individual translations $\beta \mapsto \alpha + \beta$ have been substituted by the “actions” $x \mapsto \alpha.x$.

In the traditional setting, perfect nonlinearity is closely related to bent functions (4; 12; 5): a function $\phi : G \rightarrow \mathbb{C}$ is called bent if the magnitude of its discrete Fourier transform is constant equals to $|G|$, the cardinality of the (finite abelian) group G . In this paper we present a very natural way to extend this definition by considering \mathcal{H} -valued rather than \mathbb{C} -valued functions (defined on G) where \mathcal{H} is a finite-dimensional hermitian space *i.e.* a finite-dimensional complex vector space equipped with an inner-product: such a function ϕ is called *multidimensional bent* if the square of the norm (that comes from the inner-product) of the vector in \mathcal{H} corresponding to the Fourier transform of each component functions of ϕ is constant equals to $|G|$. In other words, we replace the complex modulus by the norm of \mathcal{H} by respect to its inner-product.

Finally we show that G -perfect nonlinearity can be characterized in terms of multidimensional bentness for a particular vector space \mathcal{H} . More formally we prove that a function $f : X \rightarrow H$ is G -perfect nonlinear (where G acts on X) if and only if for all nontrivial character χ of H , the map $\phi(\chi \circ f) : G \rightarrow \mathbb{C}[X]$, where $\mathbb{C}[X]$ is the vector space of \mathbb{C} -valued functions defined on X , which is defined for $\alpha \in G$ by $x \mapsto \chi \circ f(\alpha.x) \in \mathbb{C}[X]$, is multidimensional bent.

2 Bentness and perfect nonlinearity: the classical approach

The concept of bentness was originally and independently introduced by Dillon (4) and Rothaus (12). A function $f : \mathbb{Z}_2^m \leftrightarrow \mathbb{Z}_2$ is *bent* if for all nonzero α in \mathbb{Z}_2^m ,

$$\sum_{x \in \mathbb{Z}_2^m} (-1)^{f(x) \oplus \alpha.x} = \pm 2^{\frac{m}{2}} \quad (1)$$

where “ \oplus ” denotes the modulo-2 sum and “.” the dot-product of \mathbb{Z}_2^m .

Allowing groups to be more general than the simple abelian 2-groups, Logachev, Salnikov and Yashchenko (5) generalized this notion. In order to understand it, we need to recall the theory of characters and the definition of the (discrete) Fourier transform.

By convention, when G is an additive (resp. multiplicative) group, its identity element is designed by 0_G (resp. 1_G). The neutral element for the multiplication

law of a unitary ring A is also designed by 1_A .

Let G be a finite abelian group. The *characters* of G are the group homomorphisms from G to the unit circle \mathcal{S} of the complex field \mathbb{C} . When equipped with the point-wise multiplication of functions, the set of all characters \widehat{G} is a group isomorphic to G itself. In the remainder of this contribution, we always suppose some isomorphism from G to \widehat{G} to be fixed and we denote by χ_G^α the image of $\alpha \in G$ in \widehat{G} by this isomorphism.

Now let $\phi : G \rightarrow \mathbb{C}$. Its *Fourier transform* is the map $\widehat{\phi}$ defined as

$$\begin{aligned} \widehat{\phi} : G &\rightarrow \mathbb{C} \\ \alpha &\mapsto \sum_{x \in G} \phi(x) \chi_G^\alpha(x) . \end{aligned} \tag{2}$$

Definition 1 *Let G be a finite abelian group. A function $\phi : G \rightarrow \mathcal{S}$ is called bent (by respect to the theory of Logachev, Salnikov and Yashchenko) if for all nonzero $\alpha \in G$,*

$$|\widehat{\phi}(\alpha)|^2 = |G| \tag{3}$$

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

In the sequel, we use the convenient notation G^* to denote the set of all nonidentity elements of a group G .

This notion of bentness is closely related to the concept of perfect nonlinearity introduced by Nyberg (11).

Definition 2 *Let G and H be two finite groups (respectively in multiplicative and additive representations). A function $f : G \rightarrow H$ is perfect nonlinear if for all $\alpha \in G^*$ and for all $\beta \in H$,*

$$|\{x \in X | f(\alpha x) - f(x) = \beta\}| = \frac{|G|}{|H|} . \tag{4}$$

Recently, Carlet and Ding (2) and Pott (10) discovered a characterization of bentness in the abelian groups setting in terms of bent functions that generalizes a classical result of Dillon.

Theorem 3 (2; 10) *Let G and H be two finite abelian groups. A map $f : G \rightarrow H$ is perfect nonlinear if and only if for all $\beta \in H^*$, the map $\chi_H^\beta \circ f : G \rightarrow \mathcal{S}$ is bent.*

3 Bentness and perfect nonlinearity: the group actions approach

Embedded in the definition of perfect nonlinearity is the left-regular action of a group G on itself by multiplication. This kind of operation is a particular instance of group actions. So it is possible to refine the notion of perfect nonlinearity (and, by duality through the Fourier transform, of bentness) as it has been already done in (6; 7).

Let G be a group and X a nonempty set. A *group action* of G on X is a group homomorphism Φ from G to $S(X)$, the symmetric group of X . It is called *faithful* when Φ is an injective map. Instead of writing “ $\Phi(\alpha)(x)$ ” for $(\alpha, x) \in G \times X$, we use the convenient notation “ $\alpha.x$ ”.

The action of G on itself by translation (or multiplication) is the group action used in the definitions of perfect nonlinearity and bentness (by duality). But one can naturally replace it by any group action.

Definition 4 *Let G be a finite group acting at least faithfully on a finite nonempty set X and H a finite group in additive representation. A function $f : X \rightarrow H$ is called G -perfect nonlinear if for all $\alpha \in G^*$ and for all $\beta \in H$,*

$$|\{x \in X | f(\alpha.x) - f(x) = \beta\}| = \frac{|X|}{|H|} . \quad (5)$$

If the group action is not faithful then it exists at least one $\alpha \in G^*$ such that for all $x \in X$, $\alpha.x = x$ and then no function from X to H can be G -perfect nonlinear (except in some trivial cases: G or H is (isomorphic to) the trivial group $\{0\}$).

In (6; 7), we show the following characterization of G -perfect nonlinearity.

Theorem 5 (6; 7) *Let G and H be two finite abelian groups. Let suppose that G acts faithfully on a finite nonempty set X . A map $f : X \rightarrow H$ is G -perfect nonlinear if and only if $\forall \beta \in H^*, \forall \alpha \in G$,*

$$\frac{1}{|X|} \sum_{x \in X} |(\widehat{\chi_H^\beta \circ f_{(x)}})(\alpha)|^2 = |G| \quad (6)$$

where for each $x \in X$, we have

$$\begin{aligned} f_{(x)} : G &\rightarrow H \\ \alpha &\mapsto f(\alpha.x) . \end{aligned} \quad (7)$$

Now let introduce the concept of G -bentness.

Definition 6 Let G be a finite abelian group acting at least faithfully on a finite nonempty set X . Let $\phi : X \rightarrow \mathcal{S}$. The map ϕ is called G -bent if for all $\alpha \in G^*$,

$$\frac{1}{|X|} \sum_{x \in X} |\widehat{\phi_{(x)}}(\alpha)|^2 = |G| \quad (8)$$

with for each $x \in X$,

$$\begin{aligned} \phi_{(x)} : G &\rightarrow \mathcal{S} \\ \alpha &\mapsto \phi(\alpha.x) . \end{aligned} \quad (9)$$

Informally, according to this definition, we can say that a map is G -bent if the sequence of functions $\{\phi_{(x)}\}_{x \in X}$ from G to \mathcal{S} is bent in average over all $x \in X$.

Then using the notion of G -bentness, we can rewrite theorem 5 in a form similar to theorem 3.

Theorem 7 Let G and H be two finite abelian groups. Let suppose that G acts faithfully on a finite nonempty set X . A map $f : X \rightarrow H$ is G -perfect nonlinear if and only if $\forall \beta \in H^*$, the map $\chi_H^\beta \circ f : X \rightarrow \mathcal{S}$ is G -bent.

Note that in (3; 8), we have proved the existence of a G -perfect nonlinear function $f : X \rightarrow H$ such that it exists at least one $x_0 \in X$ for which $f_{(x_0)} : G \rightarrow H$ is not classical perfect nonlinear. It ensures the fact that the group actions and the traditional versions of perfect nonlinearity are different.

In this paper, we present a second characterization of G -perfect nonlinearity in terms of a new concept called *multidimensional bentness*.

4 Multidimensional bentness

4.1 Component-wise Fourier transform

In this fourth section, G is a finite abelian group (in a multiplicative representation) and \mathcal{H} is a finite-dimensional complex vector space equipped with an inner-product $\langle \cdot, \cdot \rangle_{\mathcal{H}}$ (linear in the first variable and anti-linear in the second) i.e. \mathcal{H} is a Hermitian space. Its dimension over \mathbb{C} as a vector space is designed by $\dim_{\mathbb{C}}(\mathcal{H})$. The *norm* of \mathcal{H} by respect to the inner-product is defined for

$u \in \mathcal{H}$ as

$$\|u\|_{\mathcal{H}}^2 = \langle u, u \rangle_{\mathcal{H}}. \quad (10)$$

We fix B as an orthogonal basis (by respect to $\langle \cdot, \cdot \rangle_{\mathcal{H}}$) of \mathcal{H} and we use it to define a *component-wise multiplication*. For $(u, v) \in \mathcal{H}^2$, we have

$$u.v = \sum_{e \in B} u_e v_e e \quad (11)$$

with $u = \sum_{e \in B} u_e e$ and $v = \sum_{e \in B} v_e e$ the decompositions of u and v in the basis B .

Equipped with this multiplication \mathcal{H} becomes a unitary abelian ring (the unit is $1_{\mathcal{H}} = \sum_{e \in B} e$). It is obviously not a field but the multiplicative group of invertible elements of \mathcal{H} is $\{u \in \mathcal{H} | \forall e \in B, u_e \neq 0\}$ and the inverse of an element u of this set is simply $u^{-1} = \sum_{e \in B} u_e^{-1} e$.

The (*component-wise*) *conjugate* of $u \in \mathcal{H}$ is given by $\bar{u} = \sum_{e \in B} \bar{u}_e e$. Using conjugation and multiplication over \mathcal{H} , we also define a *component-wise norm* of $u \in \mathcal{H}$ as $u.\bar{u} = \sum_{e \in B} |u_e|^2 e$. This “norm” can be connected to the classical norm.

$$\begin{aligned} \langle u.\bar{u}, 1_{\mathcal{H}} \rangle_{\mathcal{H}} &= \left\langle \sum_{e \in B} |u_e|^2 e, \sum_{e' \in B} e' \right\rangle_{\mathcal{H}} \\ &= \sum_{e \in B} |u_e|^2 \sum_{e' \in B} \langle e, e' \rangle_{\mathcal{H}} \\ &= \sum_{e \in B} |u_e|^2 \|e\|_{\mathcal{H}}^2 \\ &\quad (\text{since } B \text{ is an orthogonal basis}) \\ &= \|u\|_{\mathcal{H}}^2. \end{aligned} \quad (12)$$

Finally we define the *unit sphere* of \mathcal{H} by

$$\mathcal{S}(\mathcal{H}) = \{u \in \mathcal{H} | \langle u.\bar{u}, 1_{\mathcal{H}} \rangle_{\mathcal{H}} = 1\} = \{u \in \mathcal{H} | \|u\|_{\mathcal{H}}^2 = 1\}. \quad (13)$$

Our objective is to introduce a notion of bentness for functions defined on the (finite abelian) group G and with values in \mathcal{H} , thus we need to define a Fourier transform to deal with this kind of maps.

Definition 8 *The component-wise Fourier transform of $\phi : G \rightarrow \mathcal{H}$ is defined as*

$$\begin{aligned} \widehat{\phi} : G &\rightarrow \mathcal{H} \\ \alpha &\mapsto \sum_{e \in B} \widehat{\phi}_e(\alpha) e \end{aligned} \quad (14)$$

where ϕ_e is the component function by respect to e i.e. for each $x \in G$

$$\phi_e(x) = (\phi(x))_e \text{ and in particular } \phi(x) = \sum_{e \in B} \phi_e(x) e . \quad (15)$$

One can note that for each $e \in B$, by unicity of a decomposition in B , $\widehat{\phi}_e = \widehat{\phi}_e$. This relation explains the abuse of notation used to denote this component-wise Fourier transform. If \mathcal{H} reduces to \mathbb{C} , classical and component-wise versions of the Fourier transform are identical.

The component-wise Fourier transform has many properties that come from the discrete Fourier transform. For instance, we have for $\alpha \in G$ and $\phi : G \rightarrow \mathcal{H}$,

$$\widehat{\widehat{\phi}}(\alpha) = |G| \phi(-\alpha) . \quad (16)$$

We can prove it by using the same well-known identical relation for the discrete Fourier transform on each component functions of ϕ and the relation $\widehat{\widehat{\phi}}_e = \widehat{\phi}_e$. From this equality and the inversion formula of the discrete Fourier transform, we deduce the *inversion formula* in the component-wise setting.

Proposition 9 *Let $\phi : G \rightarrow \mathcal{H}$. We have for each $x \in G$,*

$$\phi(x) = \frac{1}{|G|} \sum_{e \in B} \sum_{\alpha \in G} \widehat{\phi}_e(\alpha) \overline{\chi_G^\alpha(x)} e = \frac{1}{|G|} \sum_{\alpha \in G} (\widehat{\phi}(\alpha) \cdot \overline{\chi_G^\alpha(x)} 1_{\mathcal{H}}) . \quad (17)$$

This transform also satisfies the Parseval equation. In order to show this we first introduce the *component-wise convolutional product* of $(\phi, \psi) \in (\mathcal{H}^G)^2$. It is defined for $\alpha \in G$ by

$$(\phi \star \psi)(\alpha) = \sum_{e \in B} (\phi_e \star \psi_e)(\alpha) e \quad (18)$$

where the symbol “ \star ” denotes the classical (one-dimensional) convolutional product defined for $(f, g) \in (\mathbb{C}^G)^2$ by

$$(f \star g)(\alpha) = \sum_{x \in G} f(x) g(x^{-1} \alpha) . \quad (19)$$

By recalling that $\widehat{(f * g)}(\alpha) = \widehat{f}(\alpha)\widehat{g}(\alpha)$, we easily prove that

$$\widehat{(\phi \star \psi)}(\alpha) = \widehat{\phi}(\alpha) \cdot \widehat{\psi}(\alpha) . \quad (20)$$

Let $i_G : G \rightarrow G$ such that $i_G(x) = x^{-1}$ and for $f : G \rightarrow \mathbb{C}$, one defines $\overline{f} : G \rightarrow \mathbb{C}$ such that $\overline{f}(x) = \overline{f(x)}$. This last notation is generalized component-by-component to the case of functions from G to \mathcal{H} . Let us compute $\widehat{\overline{f} \circ i_G}(\alpha)$ for $\alpha \in G$.

$$\begin{aligned} \widehat{\overline{f} \circ i_G}(\alpha) &= \sum_{x \in G} \overline{f} \circ i_G(x) \chi_G^\alpha(x) \\ &= \sum_{x \in G} \overline{f(x^{-1})} \chi_G^\alpha(x) \\ &= \sum_{y \in G} \overline{f(y)} \chi_G^\alpha(y^{-1}) \\ &= \sum_{y \in G} \overline{f(y)} \chi_G^{\alpha^{-1}}(y) \\ &= \sum_{y \in G} \overline{f(y)} \overline{\chi_G^\alpha(y)} \\ &= \overline{\sum_{y \in G} f(y) \chi_G^\alpha(y)} \\ &= \overline{\widehat{f}(\alpha)} . \end{aligned} \quad (21)$$

Let $\phi : G \rightarrow \mathcal{H}$. Let us also compute $\widehat{\overline{\phi} \circ i_G}(\alpha)$ for $\alpha \in G$.

$$\begin{aligned} \widehat{\overline{\phi} \circ i_G}(\alpha) &= \sum_{e \in B} \widehat{(\overline{\phi} \circ i_G)_e}(\alpha) e \\ &= \sum_{e \in B} \widehat{(\overline{\phi \circ i_G})_e}(\alpha) e \\ &= \sum_{e \in B} \widehat{\overline{\phi_e \circ i_G}}(\alpha) e \\ &= \sum_{e \in B} \overline{\widehat{\phi_e}(\alpha)} e \\ &\quad \text{(according to (21))} \\ &= \overline{\widehat{\phi}(\alpha)} . \end{aligned} \quad (22)$$

Now let us compute $(\psi \star \overline{\psi} \circ i_G)(1_G)$ for $(\phi, \psi) \in (\mathcal{H}^G)^2$. There are two ways to find the result. The first one is given by definition of the component-wise

convolutional product.

$$\begin{aligned}
(\psi \star \bar{\psi} \circ i_G)(1_G) &= \sum_{e \in B} (\phi_e * (\bar{\psi} \circ i_G)_e)(1_G)e \\
&= \sum_{e \in B} (\phi_e * \bar{\psi}_e \circ i_G)(1_G)e \\
&= \sum_{e \in B} \sum_{x \in G} \phi_e(x) \bar{\psi}_e(x) e \\
&= \sum_{x \in X} \phi(x) \cdot \overline{\psi(x)} .
\end{aligned} \tag{23}$$

We use the inversion formula for the second way.

$$\begin{aligned}
(\phi \star \psi)(1_G) &= \frac{1}{|G|} \sum_{\alpha \in G} (\widehat{\phi \star \bar{\psi} \circ i_G})(\alpha) \cdot \overline{\chi_G^\alpha(1_G)} 1_{\mathcal{H}} \\
&= \frac{1}{|G|} \sum_{\alpha \in G} (\widehat{\phi}(\alpha) \cdot \widehat{\bar{\psi} \circ i_G}(\alpha)) \cdot 1_{\mathcal{H}} \\
&\quad \text{(according to (20))} \\
&= \frac{1}{|G|} \sum_{\alpha \in G} \widehat{\phi}(\alpha) \cdot \overline{\widehat{\psi}(\alpha)} \\
&\quad \text{(according to (22).)}
\end{aligned} \tag{24}$$

Using (23) we obtain

$$\sum_{x \in X} \phi(x) \cdot \overline{\psi(x)} = \frac{1}{|G|} \sum_{\alpha \in G} \widehat{\phi}(\alpha) \cdot \overline{\widehat{\psi}(\alpha)} \tag{25}$$

which is traditionally known as Plancherel relation when $\mathcal{H} = \mathbb{C}$. This relation is then used to obtain Parseval equation.

Theorem 10 *Let $\phi : G \rightarrow \mathcal{H}$. We have*

$$\sum_{x \in G} \sum_{e \in B} |\phi_e(x)|^2 e = \frac{1}{|G|} \sum_{\alpha \in G} \sum_{e \in B} |\widehat{\phi}_e(\alpha)|^2 e . \tag{26}$$

In particular ϕ also satisfies

$$\sum_{x \in G} \|\phi(x)\|_{\mathcal{H}}^2 = \frac{1}{|G|} \sum_{\alpha \in G} \|\widehat{\phi}(\alpha)\|_{\mathcal{H}}^2 . \tag{27}$$

And if ϕ is $\mathcal{S}(\mathcal{H})$ -valued the following formula holds

$$\sum_{\alpha \in G} \|\widehat{\phi}(\alpha)\|_{\mathcal{H}}^2 = |G|^2 . \tag{28}$$

PROOF. According to (25), we have

$$\begin{aligned} \sum_{x \in X} \phi(x) \cdot \overline{\phi(x)} &= \frac{1}{|G|} \sum_{\alpha \in G} \widehat{\phi}(\alpha) \cdot \overline{\widehat{\phi}(\alpha)} \\ \Leftrightarrow \sum_{x \in X} \sum_{e \in B} |\phi_e(x)|^2 e &= \frac{1}{|G|} \sum_{\alpha \in G} \sum_{e \in B} |\widehat{\phi}_e(\alpha)|^2 e. \end{aligned} \quad (29)$$

Then we also have

$$\begin{aligned} \langle \sum_{x \in X} \sum_{e \in B} |\phi_e(x)|^2 e, 1_{\mathcal{H}} \rangle_{\mathcal{H}} &= \langle \frac{1}{|G|} \sum_{\alpha \in G} \sum_{e \in B} |\widehat{\phi}_e(\alpha)|^2 e, 1_{\mathcal{H}} \rangle_{\mathcal{H}} \\ \Leftrightarrow \sum_{x \in X} \sum_{e \in B} |\phi_e(x)|^2 \langle e, 1_{\mathcal{H}} \rangle_{\mathcal{H}} &= \frac{1}{|G|} \sum_{\alpha \in G} \sum_{e \in B} |\widehat{\phi}_e(\alpha)|^2 \langle e, 1_{\mathcal{H}} \rangle_{\mathcal{H}} \\ \Leftrightarrow \sum_{x \in X} \sum_{e \in B} |\phi_e(x)|^2 \|e\|_{\mathcal{H}}^2 &= \frac{1}{|G|} \sum_{\alpha \in G} \sum_{e \in B} |\widehat{\phi}_e(\alpha)|^2 \|e\|_{\mathcal{H}}^2 \\ \Leftrightarrow \sum_{x \in G} \|\phi(x)\|_{\mathcal{H}}^2 &= \frac{1}{|G|} \sum_{\alpha \in G} \|\widehat{\phi}(\alpha)\|_{\mathcal{H}}^2. \end{aligned} \quad (30)$$

The last equality of the theorem is obvious. \square

4.2 Multidimensional bent functions

An appropriate notion of bentness occurs naturally in this setting.

Definition 11 *Let $\phi : G \rightarrow \mathcal{S}(\mathcal{H})$. This function is (multidimensional) bent if for all $\alpha \in G$, we have*

$$\|\widehat{\phi}(\alpha)\|_{\mathcal{H}}^2 = |G| \quad (31)$$

or in other words

$$\sum_{e \in B} |\widehat{\phi}_e(\alpha)|^2 \|e\|_{\mathcal{H}}^2 = |G|. \quad (32)$$

Such notion as been previously introduced in (9) but in a slightly different way. Another bentness notion, based on the component-wise norm, can be introduced in a way as natural as the previous one.

Definition 12 *Let $\phi : G \rightarrow \mathcal{H}$. This function is component-wise bent if*

- (1) $\forall x \in G, \phi(x) \cdot \overline{\phi(x)} = 1_{\mathcal{H}}$ (or equivalently, $\forall x \in G$ and $\forall e \in B, \phi_e(x) \in \mathcal{S}$);

(2) $\forall \alpha \in G, \widehat{\phi}(\alpha) \cdot \overline{\widehat{\phi}(\alpha)} = |G|1_{\mathcal{H}}$ (or equivalently, $\forall \alpha \in G, \forall e \in B, \phi_e$ is bent).

Obviously a function ϕ is component-wise bent if and only if each of its component functions are bent. Moreover if $\dim_{\mathbb{C}}(\mathcal{H}) = 1$ the two concepts coincide with the classical bentness notion of Logachev, Salnikov and Yashchenko. Nevertheless we will show in the sequel that component-wise and multidimensional bentness are two different notions. However there is a relation between the two approaches.

Lemma 13 *Let $\phi : G \rightarrow \mathcal{H}$ such that $\forall x \in G, \phi(x) \cdot \overline{\phi(x)} = 1_{\mathcal{H}}$ then $\phi(x) \in \mathcal{S}(\mathcal{H})$ for all $x \in G$ if and only if $\|1_{\mathcal{H}}\|_{\mathcal{H}}^2 = \sum_{e \in B} \|e\|_{\mathcal{H}}^2 = 1$.*

PROOF. Let $x \in G$. We have

$$\langle \phi(x) \cdot \overline{\phi(x)}, 1_{\mathcal{H}} \rangle_{\mathcal{H}} = \|\phi(x)\|_{\mathcal{H}}^2 = \sum_{e \in B} |\phi_e(x)|^2 \|e\|_{\mathcal{H}}^2 = \sum_{e \in B} \|e\|_{\mathcal{H}}^2 = \|1_{\mathcal{H}}\|_{\mathcal{H}}^2 \quad (33)$$

The result immediately follows. \square

According to the lemma above, if the basis B is orthogonal (and $\dim_{\mathbb{C}}(\mathcal{H}) > 1$), we can not find a function $\phi : G \rightarrow \mathcal{H}$ such that it satisfies at the same time $\forall x \in G, \phi(x) \cdot \overline{\phi(x)} = 1_{\mathcal{H}}$ and $\phi(x) \in \mathcal{S}(\mathcal{H})$. So in this particular case, component-wise and multidimensional bentness are different. Now we exhibit a relation when $\|1_{\mathcal{H}}\|_{\mathcal{H}}^2 = 1$.

Proposition 14 *Let suppose that $\|1_{\mathcal{H}}\|_{\mathcal{H}}^2 = \sum_{e \in B} \|e\|_{\mathcal{H}}^2 = 1$. Let $\phi : G \rightarrow \{u \in \mathcal{H} | u \cdot \bar{u} = 1_{\mathcal{H}}\}$. If ϕ is component-wise bent then it is also multidimensional bent.*

PROOF. According to lemma 13, $\forall x \in G, \phi(x) \in \mathcal{S}(\mathcal{H})$. Moreover we have for $\alpha \in G$,

$$\|\widehat{\phi}(\alpha)\|_{\mathcal{H}}^2 = \langle \widehat{\phi}(\alpha) \cdot \overline{\widehat{\phi}(\alpha)}, 1_{\mathcal{H}} \rangle_{\mathcal{H}} = \langle |G|1_{\mathcal{H}}, 1_{\mathcal{H}} \rangle_{\mathcal{H}} = |G| \|1_{\mathcal{H}}\|_{\mathcal{H}}^2 = |G|. \quad \square(34)$$

We will see in the sequel that although if $\|1_{\mathcal{H}}\|_{\mathcal{H}}^2 = 1$, we can find a multidimensional bent function which is not component-wise bent.

In a very similar way as for Logachev, Salnikov and Yashchenko's bent functions, it is possible to determine a combinatorial characterization of this notion using the derivative and balancedness.

Definition 15 A function $f : G \rightarrow \mathbb{C}$ is balanced if $\sum_{x \in G} f(x) = 0$.

The *derivative* of $f : G \rightarrow \mathbb{C}$ in $\alpha \in G$ is defined as

$$\begin{aligned} d_\alpha f : G &\rightarrow \mathbb{C} \\ x &\mapsto f(\alpha x) \overline{f(x)} . \end{aligned} \tag{35}$$

Then the (*component-wise*) derivative of $\phi : G \rightarrow \mathcal{H}$ is simply defined as

$$\begin{aligned} D_\alpha \phi : G &\rightarrow \mathcal{H} \\ x &\mapsto \sum_{e \in B} d_\alpha \phi_e(x) e . \end{aligned} \tag{36}$$

In particular, $(D_\alpha \phi)_e = d_\alpha \phi_e$.

A result by Logachev, Salnikov and Yashchenko gives a link between bentness, derivatives and balancedness.

Theorem 16 (5) A function $f : G \rightarrow \mathcal{S}$ is bent if and only if for all $\alpha \in G^*$, the derivative $d_\alpha f$ is balanced.

Our ambition is now to present a similar result for the multidimensional bentness.

Lemma 17 Let $\phi : G \rightarrow \mathcal{H}$. One defines the auto-correlation function of ϕ by

$$\begin{aligned} AC_\phi : G &\rightarrow \mathcal{H} \\ \alpha &\mapsto \widehat{D_\alpha \phi}(1_G) = \sum_{e \in B} \widehat{d_\alpha \phi_e}(1_G) e . \end{aligned} \tag{37}$$

Then for all $\alpha \in G$,

$$\widehat{AC_\phi}(\alpha) = \widehat{\phi}(\alpha) \cdot \overline{\widehat{\phi}(\alpha)} . \tag{38}$$

PROOF. For $\alpha \in G$, we have

$$\begin{aligned}
AC_\phi(\alpha) &= \sum_{e \in B} \widehat{d_\alpha \phi_e}(1_G) e \\
&= \sum_{e \in B} \sum_{x \in G} d_\alpha \phi_e(x) e \\
&= \sum_{e \in B} \sum_{x \in G} \phi_e(\alpha x) \overline{\phi_e(x)} e \\
&= \sum_{e \in B} \sum_{y \in G} \phi_e(\alpha y^{-1}) \overline{\phi_e(y^{-1})} e \\
&= \sum_{e \in B} (\phi_e * \overline{\phi_e} \circ i_G)(\alpha) e \\
&= (\phi \star \overline{\phi} \circ i_G)(\alpha) .
\end{aligned} \tag{39}$$

Then using relations (20) and (22) we obtain

$$\widehat{AC_\phi}(\alpha) = (\phi \star \overline{\phi} \circ i_G)(\alpha) = \widehat{\phi}(\alpha) \cdot \overline{\widehat{\phi}(\alpha)} . \quad \square \tag{40}$$

Before presenting the expected result, we give two technical lemmas. The proof of the first one can be found in (2).

Lemma 18 (2) *Let $f : G \rightarrow \mathbb{C}$. Then $f(x) = 0$ for all $x \in G^*$ if and only if $\widehat{f}(\alpha) = f(1_G)$ for all $\alpha \in G$.*

Lemma 19 *Let $\phi : G \rightarrow \mathcal{H}$ and $u \in \mathcal{H}$. We define*

$$\begin{aligned}
P_u(\phi) : G &\rightarrow \mathbb{C} \\
x &\mapsto \langle \phi(x), u \rangle_{\mathcal{H}} .
\end{aligned} \tag{41}$$

Then for all $\alpha \in G$, we have

$$\widehat{P_u(\phi)}(\alpha) = P_u(\widehat{\phi})(\alpha) = \langle \widehat{\phi}(\alpha), u \rangle_{\mathcal{H}} . \tag{42}$$

PROOF.

$$\begin{aligned}
\widehat{P_u(\phi)}(\alpha) &= \sum_{x \in G} P_u(\phi)(x) \chi_G^\alpha(x) \\
&= \sum_{x \in G} \langle \phi(x), u \rangle_{\mathcal{H}} \chi_G^\alpha(x) \\
&= \sum_{x \in G} \langle \sum_{e \in B} \phi_e(x) e, u \rangle_{\mathcal{H}} \chi_G^\alpha(x) \\
&= \langle \sum_{x \in G} \sum_{e \in B} \chi_G^\alpha(x) \phi_e(x) e, u \rangle_{\mathcal{H}} \\
&= \langle \sum_{e \in B} \widehat{\phi_e}(\alpha) e, u \rangle_{\mathcal{H}} \\
&= \langle \widehat{\phi}(\alpha), u \rangle_{\mathcal{H}} . \quad \square
\end{aligned} \tag{43}$$

The combinatorial characterization for multidimensional bentness is given by the following result.

Theorem 20 *Let $\phi : G \rightarrow \mathcal{S}(\mathcal{H})$. The function ϕ is multidimensional bent if and only if for all $\alpha \in G^*$, the map $P_{1_{\mathcal{H}}}(D_\alpha \phi) : G \rightarrow \mathbb{C}$ defined for $x \in G$ by $P_{1_{\mathcal{H}}}(D_\alpha \phi)(x) = \langle D_\alpha \phi(x), 1_{\mathcal{H}} \rangle_{\mathcal{H}}$ is balanced.*

$$\begin{aligned}
\textbf{PROOF.} \quad & \text{The map } P_{1_{\mathcal{H}}}(D_\alpha \phi) \text{ is balanced for all } \alpha \in G^* \\
& \Leftrightarrow \forall \alpha \in G^*, \sum_{x \in G} P_{1_{\mathcal{H}}}(D_\alpha \phi)(x) = 0 \\
& \Leftrightarrow \forall \alpha \in G^*, \sum_{x \in G} \langle D_\alpha \phi(x), 1_{\mathcal{H}} \rangle_{\mathcal{H}} = 0 \\
& \Leftrightarrow \forall \alpha \in G^*, \langle \sum_{x \in G} D_\alpha \phi(x), 1_{\mathcal{H}} \rangle_{\mathcal{H}} = 0 \\
& \Leftrightarrow \forall \alpha \in G^*, \langle \widehat{AC_\phi}(\alpha), 1_{\mathcal{H}} \rangle_{\mathcal{H}} = 0 \\
& \Leftrightarrow \forall \alpha \in G^*, P_{1_{\mathcal{H}}}(\widehat{AC_\phi})(\alpha) = 0 \\
& \Leftrightarrow \forall \alpha \in G, P_{1_{\mathcal{H}}}(\widehat{AC_\phi})(\alpha) = P_{1_{\mathcal{H}}}(AC_\phi)(1_G) \text{ (according to lemma 18).}
\end{aligned}$$

Moreover by lemma 19, we have

$$\begin{aligned}
P_{1_{\mathcal{H}}}(\widehat{AC_\phi})(\alpha) &= P_{1_{\mathcal{H}}}(\widehat{AC_\phi})(\alpha) \\
&= \langle \widehat{AC_\phi}(\alpha), 1_{\mathcal{H}} \rangle_{\mathcal{H}} \\
&= \langle \widehat{\phi}(\alpha), \widehat{\phi}(\alpha), 1_{\mathcal{H}} \rangle_{\mathcal{H}} \\
&\quad \text{(according to lemma 17)} \\
&= \| \widehat{\phi}(\alpha) \|_{\mathcal{H}}^2 .
\end{aligned} \tag{44}$$

On the other hand,

$$\begin{aligned}
P_{1_{\mathcal{H}}}(AC_{\phi})(1_G) &= \langle \sum_{e \in B} \widehat{d_{1_G} \phi_e}(1_G)e, 1_{\mathcal{H}} \rangle_{\mathcal{H}} \\
&= \langle \sum_{e \in B} \sum_{x \in G} |\phi_e(x)|^2 e, 1_{\mathcal{H}} \rangle_{\mathcal{H}} \\
&= \sum_{x \in G} |\phi_e(x)|^2 \|e\|_{\mathcal{H}}^2 \\
&= \sum_{x \in G} \|\phi(x)\|_{\mathcal{H}}^2 \\
&= |G| \text{ (since } \phi \text{ is } \mathcal{S}(\mathcal{H})\text{-valued.)}
\end{aligned} \tag{45}$$

Finally we have:

the map $P_{1_{\mathcal{H}}}(D_{\alpha}\phi)$ is balanced for all $\alpha \in G^*$

$$\Leftrightarrow \forall \alpha \in G, \|\widehat{\phi}(\alpha)\|_{\mathcal{H}}^2 = |G|$$

$\Leftrightarrow \phi$ is multidimensional bent. \square

5 G-perfect nonlinearity as a particular kind of multidimensional bentness

In this section, G is a finite abelian group in multiplicative representation and \mathcal{H} is the complex-vector space of functions from a nonempty finite set X to the complex field. This $|X|$ -dimensional vector space is denoted $\mathbb{C}[X]$. We choose as inner-product of $\mathbb{C}[X]$ the following sesquilinear form

$$\langle f, g \rangle_{\mathbb{C}[X]} = \sum_{x \in X} f(x) \overline{g(x)} \tag{46}$$

for $(f, g) \in \mathbb{C}[X]^2$. The fixed orthogonal basis of $\mathbb{C}[X]$ is given by the canonical basis of Dirac functions

$$\delta_x(y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \tag{47}$$

In particular for each $x \in X$, we have $\|\delta_x\|_{\mathbb{C}[X]}^2 = \frac{1}{|X|}$ and $\|1_{\mathbb{C}[X]}\|_{\mathbb{C}[X]}^2 = \sum_{x \in X} \|\delta_x\|_{\mathbb{C}[X]}^2$

$$\|\delta_x\|_{\mathbb{C}[X]}^2 = \frac{|X|}{|X|} = 1.$$

In this setting a map $\phi : G \rightarrow \mathcal{S}(\mathbb{C}[X])$ is multidimensional bent if for all $\alpha \in G$, $\|\widehat{\phi}(\alpha)\|_{\mathbb{C}[X]}^2 = \sum_{x \in X} |\widehat{\phi_{\delta_x}}(\alpha)|^2 \|\delta_x\|_{\mathcal{H}}^2 = \frac{1}{|X|} \sum_{x \in X} |\widehat{\phi_{\delta_x}}(\alpha)|^2 = |G|$.

We can already note that the last equality above is similar to the one given in definition 6.

Now let suppose that G acts faithfully on the set X .

For each $f \in \mathbb{C}[X]$ is associated the following map from G to $\mathbb{C}[X]$.

$$\begin{aligned} \phi(f) : G &\rightarrow \mathbb{C}[X] \\ \alpha &\mapsto \phi(f)(\alpha) = \sum_{x \in G} f_{(x)}(\alpha) \delta_x = \sum_{x \in G} f(\alpha.x) \delta_x . \end{aligned} \tag{48}$$

By unicity of the decomposition in the basis $\{\delta_x\}_{x \in X}$ of $\mathbb{C}[X]$, we have in particular for each $x \in X$, $\phi(f)_{\delta_x} = f_{(x)}$. Moreover if we suppose that f is \mathcal{S} -valued then $\phi(f)$ is $\mathcal{S}(\mathbb{C}[X])$ -valued since for each $\alpha \in G$, $\|\phi(f)(\alpha)\|_{\mathbb{C}[X]}^2 = \frac{1}{|X|} \sum_{x \in X} |\phi(f)_{\delta_x}(\alpha)|^2 = \frac{1}{|X|} \sum_{x \in X} |f_{(x)}(\alpha)|^2 = \frac{1}{|X|} \sum_{x \in X} |f(\alpha.x)|^2 = \frac{|X|}{|X|} = 1$.

Theorem 21 *Let $f : X \rightarrow \mathcal{S}$. Then f is G -bent if and only if $\phi(f)$ is multi-dimensional bent.*

PROOF. Let us compute for $\alpha \in G$, $\widehat{\phi(f)}(\alpha)$.

$$\begin{aligned} \widehat{\phi(f)}(\alpha) &= \sum_{x \in X} \widehat{\phi(f)_{\delta_x}}(\alpha) \delta_x \\ &= \sum_{x \in X} \widehat{f_{(x)}}(\alpha) \delta_x . \end{aligned} \tag{49}$$

Then we have

$$\begin{aligned} \|\widehat{\phi(f)}(\alpha)\|_{\mathbb{C}[X]}^2 &= \frac{1}{|X|} \sum_{x \in X} |\widehat{\phi(f)_{\delta_x}}(\alpha)|^2 \\ &= \frac{1}{|X|} |\widehat{f_{(x)}}(\alpha)|^2 . \end{aligned} \tag{50}$$

Finally we conclude

$$\begin{aligned}
& f \text{ is } G\text{-bent} \\
& \Leftrightarrow \forall \alpha \in G, \frac{1}{|X|} \sum_{x \in X} |\widehat{f_{(x)}}(\alpha)|^2 = |G| \\
& \Leftrightarrow \forall \alpha \in G, \|\widehat{\phi(f)}(\alpha)\|_{\mathbb{C}[X]}^2 = |G| \\
& \Leftrightarrow \phi(f) \text{ is multidimensional bent.} \quad \square
\end{aligned} \tag{51}$$

Corollary 22 *Let G and H be two finite abelian groups. Let suppose that G acts faithfully on a finite nonempty set X . The map $f : X \rightarrow H$ is G -perfect nonlinear if and only if $\forall \beta \in H^*$, the map $\phi(\chi_H^\beta \circ f) : G \rightarrow \mathcal{S}(\mathbb{C}[X])$ is multidimensional bent.*

PROOF.

$$\begin{aligned}
& \forall \beta \in H^*, \phi(\chi_H^\beta \circ f) \text{ is multidimensional bent} \\
& \Leftrightarrow \forall \beta \in H^*, \chi_H^\beta \circ f : X \rightarrow \mathcal{S} \text{ is } G\text{-bent (according to theorem 21)} \\
& \Leftrightarrow f \text{ is } G\text{-perfect nonlinear (according to theorem 7).} \quad \square
\end{aligned} \tag{52}$$

We have already mentioned that it exists a function $f : X \rightarrow H$ such that f is G -perfect nonlinear (and according to the previous corollary, $\phi(\chi^\beta \circ f)$ is multidimensional bent for each $\beta \in H^*$) and such that it exists $x_0 \in X$ for which $f_{(x_0)} : G \rightarrow H$ is not perfect nonlinear in the traditional setting. Then according to theorem 3 it exists $\beta_0 \in H^*$, such that $\widehat{\chi_H^{\beta_0} \circ f_{(x_0)}} : G \rightarrow \mathcal{S}$ is not bent *i.e.* there is an element $\alpha_0 \in G$ such that $|\widehat{\chi_H^{\beta_0} \circ f_{(x_0)}}(\alpha_0)|^2 \neq |G|$. Then $\phi(\chi_H^{\beta_0} \circ f)$ is not component-wise bent. Indeed if we suppose that $\phi(\chi_H^{\beta_0} \circ f)$ is component-wise bent then for each $x \in X$, $\phi(\chi_H^{\beta_0} \circ f)_{\delta_x} = \chi_H^{\beta_0} \circ f_{(x)}$ is bent and it would be also the case in particular for $\chi_H^{\beta_0} \circ f_{(x_0)}$. Then we have a function which is multidimensional but not component-wise bent. The reciprocal assertion of proposition 14 is then false.

References

- [1] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology 4(1) (1991) 3-72
- [2] C. Carlet, C. Ding, Highly nonlinear mappings, Journal of complexity 20(2) (2004) 205-244
- [3] J. Davis, L. Poinot, G -difference sets and G -perfect nonlinear functions, Private communications (2005)

- [4] J. F. Dillon, Elementary Hadamard difference sets, PhD Thesis, University of Maryland (1974)
- [5] O. A. Logachev, A. A. Salnikov, V. V. Yashchenko, Bent functions on a finite abelian group, *Discrete Math. Appl.* 7(6) (1997) 547-564
- [6] L. Poinot, S. Harari, Group actions based perfect nonlinearity (extended abstract), *Proceeding of Workshop on Coding and Cryptography WCC 2005*, Bergen (Norway) (2005) 335-244
- [7] L. Poinot, S. Harari, Group actions based perfect nonlinearity, *GESTS International Transactions on Computer Science and Engineering* 12(1) (2005) 1-14
- [8] L. Poinot, Non linéarité parfaite généralisée au sens des actions de groupes, contributions aux fondements de la solidité cryptographique (in english: group actions based perfect nonlinearity, contributions to the foundations of cryptographic solidity), PhD Thesis, University of South Toulon-Var (2005)
- [9] L. Poinot, Multidimensional bent functions, *GESTS International Transactions on Computer Science and Engineering* 18(1) (2005) 185-195
- [10] A. Pott, Nonlinear functions in abelian groups and relative difference sets, *Discrete Applied Mathematics* 138(1-2) (2004) 177-193
- [11] K. Nyberg, Perfect nonlinear S-boxes, *Proceeding of Eurocrypt'93*, *Lecture Notes in Computer Science* 809 (1994) 1-17
- [12] O. S. Rothaus, On bent functions. *Journal of Combinatorial Theory A* 20 (1976) 300-365