Journal of Discrete Mathematical Sciences and Cryptography

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tdmc20

Bent functions on a finite nonabelian group

Laurent Poinsot [a]

[a] Université du Sud Toulon-Var, Institut des Sciences de l'Ingénieur de Toulon et du Var, Avenue G. Pompidou, BP 56 , La Valette du Var cédex , 83162 , France

To cite this article: Laurent Poinsot (2006): Bent functions on a finite nonabelian group, Journal of Discrete Mathematical Sciences and Cryptography, 9:2, 349-364

To link to this article: http://dx.doi.org/10.1080/09720529.2006.10698084

Bent functions on a finite nonabelian group

Laurent Poinsot *

Université du Sud Toulon-Var
Institut des Sciences de l'Ingénieur de Toulon et du Var
Avenue G. Pompidou
BP 56, 83162 La Valette du Var cédex
France

Abstract

We introduce the notion of a bent function on a finite nonabelian group which is a natural generalization of the well-known notion of bentness on a finite abelian group due to Logachev, Salnikov and Yashchenko. Using the theory of linear representations and noncommutative harmonic analysis of finite groups we obtain several properties of such functions similar to the corresponding properties of traditional abelian bent functions.

Keywords and phrases : *Bent functions, finite nonabelian groups, noncommutative harmonic analysis, Fourier transform.*

1. Introduction

The introduction of Boolean bent functions by Rothaus [9], and Dillon [4] had important consequences in cryptology because this concept displays the most resistant functions against the so called differential [1], and linear [6] cryptanalysis. Allowing abelian groups to be more complex than the simple abelian 2-groups, Logachev, Salnikov and Yashchenko [5] generalized the notion of bentness. A function f from a finite abelian group G to the unit circle of the complex field T is bent if for all $\sigma \in G$,

$$|\widehat{f}(\sigma)|^2 = |G| \tag{1}$$

where $\widehat{f}$ is the (discrete) Fourier transform of f, $|z|$ is the complex modulus of $z \in \mathbb{C}$ and $|G|$ is the cardinality of G.

E-mail: poinsot@univ-tln.fr

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 9 (2006), No. 2, pp. 349–364

The objective of this paper is to present a generalization of the previous notion of bentness to the case of finite nonabelian groups. In terms of harmonic analysis, noncommutativity implies to deal with higher-dimensional complex vector spaces rather than the trivial one, $\mathbb{C}$, the complex field. In particular, the Fourier transform of a complex-valued function is no more $\mathbb{C}$-valued in this nonabelian context but its values are some linear endomorphisms. This Fourier transform is based on the theory of linear representations since the theory of characters is not sufficient to describe all of the duality of a nonabelian group. It is possible to introduce the concept of bentness on a finite nonabelian group in an intuitive way. First, let us rewrite formula (1) as follows: $\forall\, \sigma \in G$,

$$\widehat{f}(\sigma)\,\overline{\widehat{f}(\sigma)} = |G| \tag{2}$$

where $\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$.

Now let suppose G to be a finite nonabelian group. The discrete Fourier transform $\widehat{f}$ must be replaced by the representation-based Fourier transform denoted $\widetilde{f}$. This transform maps linear representations, i.e., group homomorphism ρ from G to the linear group of a finite dimensional complex vector space V, on linear endomorphisms $\widetilde{f}(\rho)$ of V. Since we now deal with linear operators rather than complex numbers, the multiplication is replaced by maps composition and the complex conjugate by the adjoint of endomorphisms. Thus in the nonabelian setting the formula (2) becomes

$$\widetilde{f}(\rho) \circ \widetilde{f}(\rho)^* = |G|\mathrm{Id}_V \tag{3}$$

where Id_V is the identity endomorphism of V.

The functions that satisfy this relation correspond to traditional bent functions but in the noncommutative case. In this paper are presented several properties of such functions which generalize the classical ones.

Outline of the paper

This paper is organized in five sections. The first one is the current introduction to this work. In Section 2 are given the most important and general notations used in this document. The third section summarizes some basics about the classical notion of commutative bentness by Logachev, Salnikov and Yashchenko. Then in Section 4, we present some harmonic analysis tools needed to develop a bentness notion in a

nonabelian group. Finally in Section 5, we introduce the generalization of bent functions in a finite nonabelian group and establish their main properties.

2. General notations

If X is a finite set, then $|X|$ is its cardinality. The symbol "$\circ$" denotes the composition of functions.

In this paper the letter "G" always stands for a finite group in a multiplicative representation and e_G denotes its identity. Moreover G^* is the set of nonidentity elements of G.

If $z \in \mathbb{C}$ then $\overline{z}$ (resp., $|z|$) is the complex conjugate (resp., complex modulus) of z. The multiplicative group of complex roots of the unity is denoted by T.

The dimension of a complex vector space V is designed by $\dim_{\mathbb{C}}(V)$, its identity map by Id_V and the vector space of all its endomorphisms is $\mathrm{End}(V)$. The adjoint of $U \in \mathrm{End}(V)$ is U^*; U is called unitary if $U \circ U^* = \mathrm{Id}_V$. The set of all unitary operators of V is denoted $T(V)$. Finally the trace of operators is simply designed by "tr".

3. Bent functions on a finite abelian group: the classical approach

In [5] Logachev, Salnikov and Yashchenko described a generalization of Boolean bentness to the case of T-valued functions defined on a finite abelian group. We briefly summarize their results in this section, highlighting the properties we generalize in the noncommutative setting. Nevertheless let us begin with some recalls about the theory of characters and the duality of finite abelian groups.

Let G be a finite abelian group. A *character* of G is a group homomorphism from G to T. The set of all characters of G, when equipped with point-wise multiplication, is a finite abelian group isomorphic to G itself; it is called the *dual group* of G and denoted $\widehat{G}$. The image of $\sigma \in G$ by such an isomorphism from G to $\widehat{G}$ is designed by χ^σ.

The (*discrete*) *Fourier transform* of a function $f : G \to \mathbb{C}$ is defined by

$$\begin{aligned} \widehat{f} \,:\, & G \to \mathbb{C} \\ & \sigma \mapsto \sum_{x \in G} f(x)\chi^\sigma(x)\,. \end{aligned} \tag{4}$$

This transform is a very powerful tool for the study of the properties of functions $f : G \to \mathbb{C}$. The result given below clearly explains it. It can be found in any books on Fourier analysis (e.g., see [7]).

Proposition 1 (*Trivialization of the Convolutional Product* [7]). *Let G be a finite abelian group and $(f, g) \in (\mathbb{C}^G)^2$. The convolutional product of f and g is defined as*

$$\begin{aligned} f * g \ : \ & G \to \mathbb{C} \\ & \sigma \mapsto \sum_{x \in G} f(x) g(x^{-1}\sigma) \, . \end{aligned} \tag{5}$$

Then for all $\sigma \in G$

$$\widehat{(f * g)}(\sigma) = \widehat{f}(\sigma)\widehat{g}(\sigma) \, . \tag{6}$$

This Fourier transform plays an essential role in the definition of bentness.

Definition 1. Let G be a finite abelian group and $f : G \to T$. The map f is *bent* if $\forall\, \sigma \in G$,

$$|\widehat{f}(\sigma)|^2 = |G| \, . \tag{7}$$

An equivalent way to characterize this notion of bentness needs to use the concepts of balancedness and derivative.

Definition 2. Let G be a finite abelian group and $f : G \to \mathbb{C}$. The map f is called *balanced* if

$$\sum_{x \in G} f(x) = 0 \, . \tag{8}$$

Definition 3. Let G be a finite group (not necessary abelian) and $f : G \to \mathbb{C}$. The *derivative* of f in direction $\sigma \in G$ is defined as

$$\begin{aligned} \frac{df}{d\sigma} \ : \ & G \to \mathbb{C} \\ & x \mapsto \overline{f(x)} f(\sigma x) \, . \end{aligned} \tag{9}$$

With these two notions it is possible to give to bentness a combinatorial presentation.

Theorem 1 ([5]). *Let G be a finite abelian group and $f : G \to T$. The map f is bent if and only if for all $\sigma \in G^*$, $\dfrac{df}{d\sigma}$ is balanced, i.e., $\forall\, \sigma \in G^*$, $\sum\limits_{x \in G} \dfrac{df}{d\sigma}(x) = 0$.*

Proof. We give here a slightly different proof than the one that can be found in [5]. In particular we use the fact — easily checkable — that a function $g : G \to \mathbb{C}$ satisfies $\widehat{g}$ is constant if and only if $g(x) = 0$ for all $x \in G^*$. We have

$$\begin{aligned} f \text{ is bent} &\Leftrightarrow \forall\, \sigma \in G,\ |\widehat{f}(\sigma)|^2 = |G| \\ &\Leftrightarrow \forall\, \sigma \in G,\ \widehat{f}(\sigma)\overline{\widehat{f}(\sigma)} = |G|. \end{aligned}$$

Moreover

$$\begin{aligned} \overline{\widehat{f}(\sigma)} &= \overline{\sum_{x\in G} f(x)\chi^\sigma(x)} = \sum_{x\in G} \overline{f(x)}\chi^\sigma(x^{-1}) \\ &= \sum_{y\in G} \overline{f(y^{-1})}\chi^\sigma(y) = \widehat{\overline{f \circ i_G}}(\sigma) \end{aligned}$$

with for $g : G \to \mathbb{C}$, $\overline{g} : G \to \mathbb{C}$ is defined by $\overline{g}(x) = \overline{g(x)}$ and

$$\begin{aligned} i_G \ :\ & G \to G \\ & x \mapsto x^{-1}. \end{aligned}$$

So we have

$$\begin{aligned} f \text{ is bent} &\Leftrightarrow \forall\, \sigma \in G,\ \widehat{f}(\sigma)\widehat{\overline{f \circ i_G}}(\sigma) = |G| \\ &\Leftrightarrow \forall\, \sigma \in G,\ \widehat{(f * \overline{f \circ i_G})}(\sigma) = |G| \\ &\quad \text{(by the trivialization of the convolutional product)} \\ &\Leftrightarrow \forall\, \sigma \in G^*,\ (f * \overline{f \circ i_G})(\sigma) = 0 \\ &\quad \text{(according to the beginning of the proof.)} \end{aligned}$$

This gives the conclusion since

$$\begin{aligned} (f * \overline{f \circ i_G})(\sigma) &= \sum_{x\in G} f(x)\overline{(f \circ i_G)(x^{-1}\sigma)} \\ &= \sum_{x\in G} f(x)\overline{f(\sigma^{-1}x)} \\ &= \sum_{y\in G} f(\sigma y)\overline{f(y)} \\ &\quad \text{(by the change of variables: } y = \sigma^{-1}x) \\ &= \sum_{y\in G} \frac{df}{d\sigma}(y)\,. \end{aligned}$$

□

In the case of functions from a finite abelian group G to another one H this combinatorial characterization leads to the important cryptographic concept of perfect nonlinearity [2, 8].

Another remarkable property concerning the theory of Logachev, Salnikov and Yashchenko is the fact that the knowledge of a bent function automatically leads to the existence (in a constructive way) of another one: its *dual*.

Theorem 2 ([5]). *Let G be a finite abelian group and $f : G \to T$ a bent function. Let define $\dot{f} : G \to \mathbb{C}$ by $\dot{f}(x) = \frac{1}{\sqrt{|G|}}\widehat{f}(x)$. Then $\dot{f}$, called dual of f, is T-valued and bent.*

Proof. Let us show that $\forall\, x \in G, \dot{f}(x) \in T$.

$$\begin{aligned} |\dot{f}(x)|^2 &= \dot{f}(x)\overline{\dot{f}(x)} = \frac{1}{\sqrt{|G|}}\widehat{f}(x)\frac{1}{\sqrt{|G|}}\overline{\widehat{f}(x)} \\ &= \frac{1}{|G|}|f(x)|^2 = \left|\frac{G}{G}\right| \qquad (\text{since } f \text{ is bent}) = 1. \end{aligned}$$

Now we prove that $\dot{f}$ is bent. Let $\sigma \in G$.

$$\widehat{\dot{f}}(\sigma) = \frac{1}{\sqrt{|G|}}\widehat{\widehat{f}}(\sigma) = \frac{|G|}{\sqrt{|G|}}f(\sigma^{-1}) = \sqrt{|G|}f(\sigma^{-1})$$

(it is easy to check that $\widehat{\widehat{f}}(\sigma) = |G|f(\sigma^{-1})$). Then we have

$$\begin{aligned} |\widehat{\dot{f}}(\sigma)|^2 &= \widehat{\dot{f}}(\sigma)\overline{\widehat{\dot{f}}(\sigma)} = \sqrt{|G|}f(\sigma^{-1})\sqrt{|G|}\,\overline{f(\sigma^{-1})} \\ &= |G||f(\sigma^{-1})|^2 = |G| \qquad (\text{because } f \text{ is } T\text{-valued}). \end{aligned}$$ □

4. Noncommutative harmonic analysis

4.1 *The theory of linear representations*

Definition 4. Let V be a finite-dimensional complex vector space. A *linear representation* of a finite group G on V is a group homomorphism from G to $GL(V)$ the linear group of V.

For each linear representation $\rho : G \to GL(V)$, it is possible to find a basis of V in which for all $x \in G$, $\rho(x)$ is a unitary operator of V, i.e., $\rho : G \to T(V)$. Indeed, we can check that for a linear representation ρ of G on V, for each $x \in G$, $\rho(x)$ leaves invariant the following inner-product in V

$$\langle u, v\rangle = \sum_{x\in G}\langle \rho(x)(u), \rho(x)(v)\rangle_V \tag{10}$$

where $(u, v) \in V^2$ and $\langle \cdot, \cdot \rangle_V$ denotes any inner-product of V (linear in the first variable and anti-linear in the second). Then in the remainder, without loss of generality, we only consider unitary representations.

The linear representations of G on $\mathbb{C}$ can be identified with the characters of G since $\mathbb{C}^*$ and $GL(\mathbb{C})$ are isomorphic. Actually if G is a finite abelian group then the notion of linear representation gives nothing new because it is equivalent to the notion of characters.

Definition 5. A linear representation ρ of a finite group G on V is said *irreducible* if there is no subspace $W \subset V$, other than $\{0_V\}$ and V, such that $\forall\, x \in G, \forall\, w \in W, \rho(x)(w) \in W$.

Definition 6. Two linear representations ρ and ρ' of a finite group G on respectively V and V' are *isomorphic* if it exists a linear isomorphism $\Phi : V \to V'$ such that for all $x \in G$,

$$\Phi \circ \rho(x) = \rho'(x) \circ \Phi\,. \tag{11}$$

The notion of isomorphism is an equivalence relation for linear representations.

Definition 7. For a finite group G, the *dual* of G, denoted $\widetilde{G}$, is a set that contains exactly one and only one representative of each equivalence class of isomorphic irreducible representations of G.

By definition, if $(\rho, \rho') \in \widetilde{G}^2$, $\rho \neq \rho'$ then ρ and ρ' are nonisomorphic irre-ducible representations of G. In the remainder, the notation

$$\rho_V \in \widetilde{G} \tag{12}$$

means that $\rho_V : G \to T(V)$ is an irreducible representation of G.

If G is a finite abelian group, then $\widetilde{G}$ is equal to $\widehat{G}$ (up to an isomorphism from $GL(\mathbb{C})$ to $\mathbb{C}^*$). If G is finite nonabelian group, the two notions of duality become distinct (in particular, $\widetilde{G}$ is not a group). By abuse of notation, $\widetilde{G}^*$ is defined as the set $\widetilde{G} \setminus \{\rho_0\}$ where ρ_0 is the *trivial* or *principal representation* of G, i.e., $\forall\, x \in G$, $\rho_0(x) = \mathrm{Id}_{\mathbb{C}}$.

When dealing with linear representations, a major result, know as Schur's lemma, should be kept in mind.

Lemma 1 ([7]). *Let G be a finite group. Let $\rho_V \in \widetilde{G}$ and $\lambda \in \mathrm{End}(V)$. If $\forall\, x \in G$, $\lambda \circ \rho_V(x) = \rho_V(x) \circ \lambda$ then λ is a multiple of the identity i.e. it exists $k \in \mathbb{C}$ such that $\lambda = k\mathrm{Id}_V$.*

As direct consequences of the Schur's lemma, we can establish the two following results that will be use in the sequel.

Lemma 2 ([7]). *Let G be a finite group. For $x \in G^*$,*

$$\sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V)\mathrm{tr}(\rho_V(x)) = 0\,. \tag{13}$$

Lemma 3. *Let G be a finite group. Let $\rho_V \in \widetilde{G}^*$. Then*

$$\sum_{x \in G} \rho_V(x) = 0_{\mathrm{End}(V)}\,. \tag{14}$$

Proof. Let $\lambda \in \mathrm{End}(V)$ defined as $\lambda = \sum_{x\in G} \rho_V(x)$. Let $x_0 \in G$. We have

$$\begin{aligned}\lambda &= \sum_{x\in G} \rho_V(x) = \sum_{x\in G} \rho_V(x_0 x)\\ &= \rho_V(x_0) \circ \sum_{x\in G} \rho_V(x) = \rho_V(x_0)\circ\lambda\end{aligned}$$

but also

$$\begin{aligned}\lambda &= \sum_{x\in G} \rho_V(x) = \sum_{x\in G} \rho_V(x x_0)\\ &= \left(\sum_{x\in G} \rho_V(x)\right)\circ \rho_V(x_0) = \lambda \circ \rho_V(x_0)\,.\end{aligned}$$

In particular $\lambda \circ \rho_V(x_0) = \rho_V(x_0)\circ\lambda$. As it is true for any $x_0 \in G$, λ commutes with all $\rho_V(x)$. By the Schur's lemma, λ is a multiple on the identity: it exists $k \in \mathbb{C}$ such that $\lambda = k\mathrm{Id}_V$. Now let suppose $\lambda \neq 0_{\mathrm{End}(V)}$, then $k \in \mathbb{C}^*$. Using the first part of the proof, we know that $\lambda = \rho_V(x)\circ\lambda$ (for each $x \in G$). Then $(\mathrm{Id}_V - \rho_V(x))\circ\lambda = 0_{\mathrm{End}(V)}$. As $\lambda = k\mathrm{Id}_V$, we have $(\mathrm{Id}_V - \rho_V(x))\circ(k\mathrm{Id}_V) = 0_{\mathrm{End}(V)}$. Since $k \neq 0$, we have $\mathrm{Id}_V - \rho_V(x) = 0_{\mathrm{End}(V)}$ or also $\rho_V(x) = \mathrm{Id}_V$ which is a contradiction with the assumption that ρ is non trivial.

4.2 *The representation-based Fourier transform*

By substituting irreducible linear representations to characters, it is possible to define a kind of Fourier transform for nonabelian groups. Let G be any finite group.

Definition 8. Let $\phi : G \to \mathbb{C}$. The (*representation-based*) *Fourier transform* of f is defined for $\rho_V \in \widetilde{G}$ as

$$\widetilde{\phi}(\rho_V) = \sum_{x\in G} \phi(x)\rho_V(x) \in \mathrm{End}(V)\,. \tag{15}$$

This Fourier transform maps a function $f \in \mathbb{C}^G$ on a function $\widetilde{f} \in \left(\bigoplus_{\rho_V \in \widetilde{G}} \mathrm{End}(V) \right)^{\widetilde{G}}$ where $\bigoplus$ denotes the (generalized) direct sum of vector spaces.

Note that this transform is defined up to the choice of a system of representatives of irreducible isomorphic linear representations. Actually the transform is defined up to a linear isomorphism between complex vector spaces, i.e., if ρ_V and $\rho_{V'}$ are two irreducible isomorphic linear representations of G then it exists a linear isomorphism $\Phi : V \to V'$ such that $\Phi^{-1} \circ \rho_{V'}(x) \circ \Phi = \rho_V(x)$ for all $x \in G$. Then for any $f : G \to \mathbb{C}$, we have $\widetilde{f}(\rho_V) = \Phi^{-1} \circ \widetilde{f}(\rho_{V'}) \circ \Phi$. Finally, up to linear isomorphisms, the Fourier transform does not depend on the choice of the representatives.

This notion is a generalization of the classical discrete Fourier transform. This transform is invertible so we have also an *inversion formula*.

Proposition 2 ([7]). *Let $\phi : G \to \mathbb{C}$. Then for all $x \in G$ we have,*

$$\phi(x) = \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x^{-1}) \circ \widetilde{\phi}(\rho_V)) \,. \tag{16}$$

A technical lemma is given below.

Lemma 4. *Let $\phi : G \to \mathbb{C}$. We have*

1. *$\phi(x) = 0 \; \forall \; x \in G^*$ if and only if $\forall \; \rho_V \in \widetilde{G}$, $\widetilde{\phi}(\rho_V) = \phi(e_G)\mathrm{Id}_V$;*
2. *$\phi(\rho_V) = 0_{\mathrm{End}(V)} \; \forall \; \rho_V \in \widetilde{G}^*$ if and only if ϕ is constant.*

Proof. 1. $\Rightarrow$) For $\rho_V \in \widetilde{G}$, we have

$$\begin{aligned} \widetilde{\phi}(\rho_V) &= \sum_{x \in G} \phi(x)\rho_V(x) && \text{(by definition)} \\ &= \phi(e_G)\rho_V(e_G) && \text{(by assumption on } \phi) \\ &= \phi(e_G)\mathrm{Id}_V && \text{(since } \rho_V \text{ is a group homomorphism).} \end{aligned}$$

$\Leftarrow$) For $x \in G$, the inversion formula gives

$$\begin{aligned} \phi(x) &= \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x^{-1}) \circ \widetilde{\phi}(\rho_V)) \\ &= \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x^{-1}) \circ \phi(e_G)\mathrm{Id}_V) \\ &\quad \text{(by hypothesis)} \end{aligned}$$

$$
\begin{aligned}
&= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x^{-1})) \\
&= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x)^{-1}) \\
&\quad \text{(since } \rho_V \text{ is a group homomorphism)} \\
&= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x)^{*}) \\
&\quad \text{(since } \rho_V(x) \text{ is unitary)} \\
&= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \overline{\mathrm{tr}(\rho_V(x))} \\
&= \frac{\phi(e_G)}{|G|} \overline{\sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x))} \\
&= 0 \text{ if } x \neq e_G \text{ (according to Lemma 2).}
\end{aligned}
$$

2. $\Rightarrow$) By the inversion formula, $\forall\, x \in G$,

$$
\begin{aligned}
\phi(x) &= \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(x^{-1}) \circ \widetilde{\phi}(\rho_V)) \\
&= \frac{1}{|G|} \mathrm{tr}(\widetilde{\phi}(\mathrm{Id}_{\mathbb{C}})) \qquad \text{(by hypothesis)}.
\end{aligned}
$$

$\Leftarrow$) Let $\rho_V \in \widetilde{G}$, we have $\widetilde{\phi}(\rho_V) = k \sum\limits_{x \in G} \rho_V(x)$ (with $\phi(x) = k\ \forall\, x \in G$).

According to Lemma 3, we deduce that $\widetilde{\phi}(\rho_V) = 0_{\mathrm{End}(V)}$ for all $\rho_V \in \widetilde{G}^*$. □

This tools from harmonic analysis will have a significant interest in the remainder of this paper for the establishment of a theory of bent functions on a finite nonabelian group similar to the one of Logachev, Salnikov and Yashchenko.

5. The main properties of bent functions

In the remainder of this section, G denotes a finite *nonabelian* group.

Definition 9. Let $f : G \to T$. The map f is called *bent* if $\forall\, \rho_V \in \widetilde{G}$,

$$\widetilde{f}(\rho_V) \circ \widetilde{f}(\rho_V)^* = |G| \mathrm{Id}_V. \tag{17}$$

This formula is very similar to the one of Logachev, Salnikov and Yashchenko (formula (7)) up to the substitution of the discrete Fourier

transform by its representation-based version, the complex multiplication by the composition, the complex conjugate by the adjoint of operators and the addition of the factor Id_V.

The Fourier transform of bent functions are no more — up to a multiplicative factor $|G| - T$-valued as in the commutative case but, again up to the same factor $|G|$, $T(V)$-valued. This is the price to pay when dealing with nonabelian groups: higher-dimensions are needed.

Using the trace of endomorphisms, we can easily check that if $f : G \to T$ is bent then for all $\rho_V \in \widehat{G}$,

$$\|\widehat{f}(\rho_V)\|_V^2 = \dim_{\mathbb{C}}(V)|G| \tag{18}$$

where for $U \in \mathrm{End}(V)$, $\|U\|_V^2 = \mathrm{tr}(U \circ U^*)$. Up to the factor $\dim_{\mathbb{C}}(V)$ which reduces to 1 when $V = \mathbb{C}$, this last formula seems identical to (7). An interesting question, left open in this paper, is to know whether or not the functions that satisfy (18) are bent.

5.1 *Derivative and bent functions*

Although the definition of noncommutative bentness seems to be quite natural, we now show that it is actually legitimate. This is done by using the notions of balancedness and derivative in a way similar to the traditional abelian setting.

Lemma 5. *Let $f : G \to \mathbb{C}$. The* autocorrelation function *of f is defined as*

$$\begin{aligned} AC_f \;:\; & G \to \mathbb{C} \\ & \sigma \mapsto \sum_{x \in G} \frac{df}{d\sigma}(x)\,. \end{aligned} \tag{19}$$

Then we have for all $\rho_V \in \widehat{G}$,

$$\widehat{AC_f}(\rho_V) = \widehat{f}(\rho_V) \circ \widehat{f}(\rho_V)^*\,. \tag{20}$$

Proof. Let $\rho_V \in \widehat{G}$. We have

$$\begin{aligned} \widehat{AC_f}(\rho_V) &= \sum_{x \in G} AC_f(x)\rho_V(x) \\ &= \sum_{x \in G}\sum_{y \in G} \frac{df}{dx}(y)\rho_V(x) \\ &= \sum_{x \in G}\sum_{y \in G} \frac{df}{dx}(y)\rho_V(xyy^{-1}) \end{aligned}$$

$$= \sum_{x\in G}\sum_{y\in G} \frac{df}{dx}(y)\rho_V(xy)\circ\rho_V(y)^*$$
$$= \sum_{y\in G}\sum_{x\in G} f(xy)\rho_V(xy)\circ\overline{f(y)}\rho_V(y)^*$$
$$= \widetilde{f}(\rho_V)\circ\widetilde{f}(\rho_V)^*. \qquad \square$$

Theorem 3. *Let $f : G \to T$. The map f is bent if and only if for all $\sigma \in \widetilde{G}^*$, $\frac{df}{d\sigma}$ is balanced.*

Proof. $\forall\, \sigma \in G^*$,

$$\begin{aligned}\frac{df}{d\sigma} \text{ is balanced } &\Leftrightarrow \forall\, \sigma \in G^*, \sum_{x\in G}\frac{df}{d\sigma}(x) = 0\\ &\Leftrightarrow \forall\, \sigma \in G^*, AC_f(\sigma) = 0\\ &\Leftrightarrow \forall\, \rho_V \in \widetilde{G}, \widetilde{AC_f}(\rho_V) = AC_f(e_G)\mathrm{Id}_V\\ &\quad \text{(according to Lemma 4)}\\ &\Leftrightarrow \forall\, \rho_V \in \widetilde{G},\ \widetilde{f}(\rho_V)\circ\widetilde{f}(\rho_V)^* = |G|\mathrm{Id}_V.\end{aligned}$$

The last equivalence comes from Lemma 5 and the fact that f is T-valued. $\square$

The result above is exactly the same as the one given in Section 3 but because it is established in the noncommutative setting we should be careful not to identify left and right multiplications. In other terms, we should prove a similar result concerning a right-derivative of $f : G \to T$; let $\sigma \in G$,

$$\begin{aligned}\frac{df}{d\sigma} \ :\ & G \to T\\ & x \mapsto \overline{f(x)}f(x\sigma)\,.\end{aligned} \tag{21}$$

However, although left and right multiplication are different, they are actually isomorphic. So the right case leads to results symmetric to the ones obtained in the left case.

5.2 *Dual bent function*

This subsection is dedicated to the question of the existence of a dual noncommutative bent function as it is the case in the abelian situation. The answer to this question needs the development of an original concept of bentness for functions $\phi : \widetilde{G} \to \bigoplus_{\rho_V\in\widetilde{G}} \mathrm{End}(V)$. In the sequel we suppose

these functions to be defined up to a linear isomorphism between vector spaces.

Definition 10. Let $\phi : \widetilde{G} \to \bigoplus_{\rho_V \in \widetilde{G}} \mathrm{End}(V)$. We define the *Fourier transform* of ϕ as

$$\begin{aligned} \check{\phi} \; : \; & G \to \mathbb{C} \\ & \sigma \mapsto \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(\sigma) \circ \phi(\rho_V)) \,. \end{aligned} \tag{22}$$

This Fourier transform is essentially the inverse Fourier transform of a function $f : G \to \mathbb{C}$. It is an invertible transform and the corresponding inversion formula is given in the following lemma.

Lemma 6 (*Inversion formula*). *Let $\phi : \widetilde{G} \to \bigoplus_{\rho_V \in \widetilde{G}} \mathrm{End}(V)$. Then for all $\rho_V \in \widetilde{G}$*

$$\phi(\rho_V) = \frac{1}{|G|} \sum_{x \in G} \check{\phi}(x) \rho_V(x)^* . \tag{23}$$

Proof. The representation-based Fourier transform is a bijective map. Then it exists one and only one $f : G \to \mathbb{C}$ such that $\widetilde{f} = \phi$. Then for $\sigma \in G$, $\check{\phi}(\sigma) = \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \mathrm{tr}(\rho_V(\sigma) \circ \widetilde{f}(\rho_V)) = |G| f(\sigma^{-1})$ according to the inversion formula of the representation-based Fourier transform. Thus for each $\sigma \in G$, $f(\sigma) = \frac{1}{|G|} \check{\phi}(\sigma^{-1})$. Finally for $\rho_V \in \widetilde{G}$,

$$\begin{aligned} \phi(\rho_V) \; &= \; \widetilde{f}(\rho_V) = \sum_{x \in G} f(x) \rho_V(x) \\ &= \; \frac{1}{|G|} \sum_{x \in G} \check{\phi}(x^{-1}) \rho_V(x) = \frac{1}{|G|} \sum_{y \in G} \check{\phi}(y) \rho_V(y)^* . \end{aligned}$$

Let us also give another technical lemma useful in the sequel.

Lemma 7. *Let $\phi : \widetilde{G} \to \bigoplus_{\rho_V \in \widetilde{G}} \mathrm{End}(V)$. We have for all $\rho_V \in \widetilde{G}$,*

$$\widetilde{\check{\phi}}(\rho_V) = |G| \phi(\rho_V^*) \,. \tag{24}$$

Proof. The representation based Fourier transform is a bijective map. Then it exists one and only one $f : G \to \mathbb{C}$ such that $\widetilde{f} = \phi$. As in the previous proof we can find that for all $\sigma \in G$,

$$\check{\phi}(\sigma) = |G| f(\sigma^{-1}) = |G| (f \circ i_G)(\sigma)$$

where $i_G(x) = x^{-1}$ for each $x \in G$. Then for $\rho_V \in \widetilde{G}$,

$$\begin{aligned}\widetilde{\check{\phi}}(\rho_V) &= |G|\widetilde{(f \circ i_G)}(\rho_V) = |G| \sum_{x\in G} f(x^{-1})\rho_V(x) \\ &= |G| \sum_{x\in G} f(x)\rho_V(x)^* \\ &= |G|\phi(\rho_V^*)\,.\end{aligned}$$

Note that ρ_V^* is (isomorphic to) an element of $\widetilde{G}$. □

Definition 11. A function $\phi : \widetilde{G} \to \bigoplus_{\rho_V\in\widetilde{G}} T(V)$ is said *bent* if for all $\sigma \in G$,

$$|\check{\phi}(\sigma)|^2 = |G|\,. \tag{25}$$

This "unnatural" definition allows us to introduce dual bentness in the nonabelian setting.

Theorem 4. *Let $f : G \to T$. Let define $\dot{f} : \widetilde{G} \to \bigoplus_{\rho_V\in\widetilde{G}} \mathrm{End}(V)$ by $\dot{f}(\rho_V) = \frac{1}{\sqrt{|G|}}\widetilde{f}(\rho_V)$ for $\rho_V \in \widetilde{G}$. Then $\dot{f}$, called* dual *of f, is $\bigoplus_{\rho_V\in\widetilde{G}} T(V)$-valued and bent.*

Proof. First let us show that $\forall\ \rho_V \in \widetilde{G}$, $\dot{f}(\rho_V) \in T(V)$.

$$\begin{aligned}\dot{f}(\rho_V) \circ \dot{f}(\rho_V)^* &= \frac{1}{\sqrt{|G|}}\widetilde{f}(\rho_V) \circ \frac{1}{\sqrt{|G|}}\widetilde{f}(\rho_V)^* \\ &= \frac{1}{|G|}\widetilde{f}(\rho_V) \circ \widetilde{f}(\rho_V)^* \\ &= \mathrm{Id}_V\end{aligned}$$

because f is bent.

Let us prove that $\dot{f}$ is bent, i.e., $\forall\ \sigma \in G$, $|\check{\dot{f}}(\sigma)|^2 = |G|$.

We have

$$\begin{aligned}\check{\dot{f}}(\sigma) &= \sum_{\rho_V\in\widetilde{G}} \dim_{\mathbb{C}}(V)\mathrm{tr}(\rho_V(\sigma) \circ \dot{f}(\rho_V)) \\ &= \frac{1}{\sqrt{|G|}} \sum_{\rho_V\in\widetilde{G}} \dim_{\mathbb{C}}(V)\mathrm{tr}(\rho_V(\sigma) \circ \widetilde{f}(\rho_V)) \\ &= \frac{|G|}{\sqrt{|G|}} f(\sigma^{-1}) \qquad \text{(by the inversion formula)} \\ &= \sqrt{|G|} f(\sigma^{-1}).\end{aligned}$$

Then

$$\begin{aligned} |\check{f}(\sigma)|^2 &= \check{f}(\sigma)\,\overline{\check{f}(\sigma)} \\ &= \sqrt{|G|}f(\sigma^{-1})\,\sqrt{|G|}\,\overline{f(\sigma^{-1})} \\ &= |G|\,|f(\sigma^{-1})|^2 = |G| \end{aligned}$$

because f is T-valued. □

We can establish a symmetric result.

Proposition 3. *Let $\phi : \widetilde{G} \to \bigoplus_{\rho_V \in \widetilde{G}} T(V)$ a bent function. Let define $\dot{\phi} : G \to \mathbb{C}$ by $\dot{\phi}(\sigma) = \frac{1}{\sqrt{|G|}}\check{\phi}(\sigma)$ for $\sigma \in G$. Then $\dot{\phi}$, called* dual *of ϕ, is T-valued and bent.*

Proof. Is $\dot{\phi}$ T-valued? Let $\sigma \in G$.

$$\begin{aligned} |\dot{\phi}(\sigma)|^2 &= \dot{\phi}(\sigma)\,\overline{\dot{\phi}(\sigma)} = \frac{1}{|G|}\check{\phi}(\sigma)\,\overline{\check{\phi}(\sigma)} \\ &= \frac{1}{|G|}|\check{\phi}(\sigma)|^2 = 1 \end{aligned}$$

because ϕ is bent.

Is $\dot{\phi}$ bent? Let $\rho_V \in \widetilde{G}$. We have

$$\widetilde{\dot{\phi}}(\rho_V) = \frac{1}{\sqrt{|G|}}\widetilde{\check{\phi}}(\rho_V) = \sqrt{|G|}\phi(\rho_V^*)$$

according to Lemma 7.

Then for all $\rho_V \in \widetilde{G}$,

$$\widetilde{\dot{\phi}}(\rho_V) \circ \widetilde{\dot{\phi}}(\rho_V)^* = |G|\phi(\rho_V^*) \circ \phi(\rho_V^*)^* = |G|\mathrm{Id}_V$$

because $\forall\ \rho_V \in \widetilde{G}$, $\phi(\rho_V) \in T(V)$. □

6. Hadamard construction

We exhibit an example of a nonabelian bent function. In order to do this, we use some combinatorial objects called *Hadamard difference sets*. We do not go into details but definitions and results can be found in [3] for instance.

Let G be a finite nonabelian group that contains a Hadamard difference set D. Let define $f : G \to \{\pm 1\} \subset T$ as $f(x) = (-1)^{i_D(x)}$ where i_D is the indicator function of D. We can check that f is a nonabelian bent

function. Indeed let compute $\widetilde{f}(\rho_V)$ for $\rho_V \in \widetilde{G}^*$.

$$\begin{aligned}\widetilde{f}(\rho_V) &= \sum_{x\in G}(-1)^{i_D(x)}\rho_V(x)\\ &= -\sum_{x\in D}\rho_V(x)+\sum_{x\in G\setminus D}\rho_V(x)\\ &= -2\sum_{x\in D}\rho_V(x)+\underbrace{\sum_{x\in G}\rho_V(x)}_{=0_{\mathrm{End}(V)} \text{ because } \rho_V \text{ is nontrivial}}.\end{aligned}$$

We now put $\rho_V(D) = \sum_{x\in D}\rho_V(x)$. Then we have $\widetilde{f}(\rho_V)\circ\widetilde{f}(\rho_V)^* = 4\rho_V(D)\circ\rho_V(D)^* = |G|\mathrm{Id}_V$ (refer to [3] for the last equality). Therefore f is nonabelian bent. By Theorem 4, its dual $\dot{f}(\rho_V) = -\frac{2}{\sqrt{|G|}}\sum_{x\in D}\rho_V(x)$ is also bent.

References

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

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

[3] J. Davis and K. Smith, A construction of difference sets in high exponent 2-groups using representation theory, *Journal of Algebraic Combinatorics*, Vol. 3 (1994), pp. 137–151.

[4] J. F. Dillon, *Elementary Hadamard Difference Sets*, Ph.D. Thesis, University of Maryland, 1974.

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

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

[7] G. Peyré, L'algèbre discrete de la transformée de Fourier, *Mathématiques à l'Université*, Ellipses, 2004.

[8] A. Pott, Nonlinear functions in abelian groups and relative difference sets, *Discrete Applied Mathematics*, Vol. 138 (1-2) (2004), pp. 177–193.

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

Received January, 2006