Non-Boolean almost perfect nonlinear functions on non-Abelian groups

Laurent Poinsot, Alexander Pott

Non-Boolean Almost Perfect Nonlinear Functions on Non-Abelian Groups

Laurent Poinsot
LIPN - UMR CNRS 7030, Institut Galilée, University Paris XIII,
99, avenue Jean-Baptiste Clment,
93430 Villetaneuse
laurent.poinsot@lipn.univ-paris13.fr

Alexander Pott
Department of Mathematics, Otto-von-Guericke-University Magdeburg,
39106 Magdeburg, Germany
alexander.pott@ovgu.de

Received (Day Month Year)
Accepted (Day Month Year)
Communicated by (xxxxxxxxxx)

The purpose of this paper is to present the extended definitions and characterizations of the classical notions of APN and maximum nonlinear Boolean functions to deal with the case of mappings from a finite group K to another one N with the possibility that one or both groups are non-Abelian.

Keywords: Almost perfect nonlinear; bent function; maximal nonlinear.

2000 Mathematics Subject Classification: 94A60, 20C05, 05B10

1. Highly nonlinear functions in the Abelian group setting

The study of nonlinear properties of Boolean functions is one of the major tasks in secret-key cryptography. But the adjective "nonlinear" has several meanings: it can be related to the resistance against the famous differential attack [2] and, in this interpretation, actually refers to (almost) perfect nonlinear functions. Moreover nonlinearity is also related to the maximum magnitude of the Fourier spectrum of Boolean functions - under the names "bent", "almost bent" or "maximal nonlinear" functions - which is itself linked to the resistance against the linear attack [17]. These two ways to define nonlinearity are not independent and even, in many situations, are exactly the same.

Most of the studies and results on nonlinearity concerns Boolean functions, or in other words, functions from K to N where K and N are both elementary Abelian 2-groups. Even if this kind of groups seems to be very natural for cryptographic purpose, there is no rule that prevent us to use more complex groups and even non-Abelian ones. In this paper, we will discuss the standard notion of nonlinearity in

the non-Abelian setting. Nevertheless we begin by some definitions and basic tools used to study nonlinearity in the Abelian case. In order to keep the paper fairly selfcontained some proofs of well-known results will be added.

Let K and N be two finite groups written multiplicatively of orders m and n respectively. Let G be the direct product $K \times N$. A mapping $f : K \to N$ is called **perfect nonlinear** (see [18]) if and only if for each $a \in K$, $a \neq 1_K$ and each $b \in N$, the quantity

$$\delta_f(a,b) = |\{g \in K | f(ag)(f(g))^{-1} = b\}| \tag{1}$$

is constant equals to $\frac{m}{n}$. In [10] the reader may find a very complete survey on the subject. In the cases where n does not divide m, it is impossible for perfect nonlinear functions to exist. We note that perfect nonlinear functions also cannot exist if K and N are elementary Abelian 2-groups of the same order. Actually, a more general result holds:

Theorem 1. *Let K be an arbitrary group of order $m = 2^a$, and let N be an Abelian group of order $n = 2^b$. A perfect nonlinear function $f : K \to N$ does not exist, if*

1. *a is odd;*
2. *$a = 2s$ is even and $b \geq s + 1$.*

For proof, we refer to [12, 16, 18]. Since perfect nonlinear functions do not exist in many cases, the following definition is meaningful: we call $f : K \to N$ an **almost perfect nonlinear** (APN) function (see [19]) if and only if

$$\sum_{(a,b)\in G} \delta_f(a,b)^2 \leq \sum_{(a,b)\in G} \delta_g(a,b)^2 \ \forall g : K \to N \ . \tag{2}$$

Both these definitions do not use the commutativity in a group. Hence these definitions also apply to the non-Abelian situation.

With each function $f : K \to N$ we associate its graph $D_f \subseteq G$:

$$D_f = \{(g, f(g)) | g \in K\} \ . \tag{3}$$

This set plays an important role in the study of nonlinear properties of the corresponding function. For instance f is perfect nonlinear if and only if its graph is a splitting $(m, n, m, \frac{m}{n})$ difference set in G relative to the normal subgroup N. Recall that a set $R \subseteq G = K \times N$ of cardinality k is a (splitting) (m, n, k, λ) difference set in G relative to N if and only if the following property holds: the list of nonidentity quotients $r(r')^{-1}$ with $r, r' \in R$ covers every element in $G \setminus \{1_K\} \times N$ precisely λ times and no element in $\{1_K\} \times (N \setminus \{1_N\})$ is covered. The term *splitting* refers to the fact that the group in which the relative difference set exists is $K \times N$, hence it "splits", where one of the factors is the "forbidden subgroup". We note that also non-splitting relative difference sets are studied, however for applications in cryptography only *mappings* $f : K \to N$ seem to be of interest, and then the graph corresponds to a splitting relative difference sets. Moreover, we have $k = m$ in this situation, and this case is called *semi-regular*. There are also many relative

difference sets known where $k \neq m$. For a survey on relative difference sets, we refer to [20].

In general such combinatorial structures are studied using the notion of group algebras. Let G be a finite group (written multiplicatively) and R a commutative ring with a unit. We denote by $R[G]$ the **group algebra** of G; its underlying R-module is free and has a basis indexed by the elements of G and which is identified to G itself: so it is a free R-module of rank $|G|$ and, as such, isomorphic to the direct sum $\bigoplus_{g\in G} R_g$ where for each $g \in G$, $R_g = R$.

Every element D of $R[G]$ can be uniquely represented as

$$D = \sum_{g\in G} d_g g, \text{ with } d_g \in R \ . \tag{4}$$

The addition in $R[G]$ is given as a component-wise addition of R. More precisely

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} (a_g + b_g)\, g \tag{5}$$

while the multiplication - convolutional product - is

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g \ . \tag{6}$$

Finally the scalar multiplication by elements of R is the usual one

$$\lambda\left(\sum_{g\in G} d_g g\right) = \sum_{g\in G} (\lambda d_g) g, \text{ with } \lambda \in R \ . \tag{7}$$

Any subset D of G is naturally identified with the following element of $R[G]$

$$\sum_{g\in G} 1_D(g) g = \sum_{g\in D} g \ , \tag{8}$$

where we define the **indicator function** of D

$$1_D(g) = \begin{cases} 1_R \text{ if } g \in D \ , \\ 0_R \text{ if } g \notin D \ . \end{cases} \tag{9}$$

When $R = \mathbb{C}$ we define

$$\left(\sum_{g\in G} d_g g\right)^{(-1)} = \sum_{g\in G} \overline{d_g} g^{-1} = \sum_{g\in G} \overline{d_{g^{-1}}} g \tag{10}$$

where $\overline{z}$ is the complex conjugate of $z \in \mathbb{C}$.
For instance for a function $f : K \to N$ and $G = K \times N$, we have

$$D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b) \in \mathbb{Z}[G] \ . \tag{11}$$

As we claimed above, (m, n, k, λ) difference sets in $G = K \times N$ relative to N have a natural interpretation in $\mathbb{Z}[G]$ because $R \subseteq G$ is such a set if and only if it satisfies the following group ring equation:

$$RR^{(-1)} = k1_G + \lambda(G - N) \ . \tag{12}$$

Therefore, we have the following well known theorem which holds in the Abelian as well as in the non-Abelian case:

Theorem 2. *A function $f : K \to N$ is perfect nonlinear if and only if the graph D_f of f is a splitting $(m, n, m, \frac{m}{n})$ difference set relative to $\{1_K\} \times N$.*

Another important tool for the study of highly nonlinear mappings - but restricted to the case of finite **Abelian** groups - is the notion of group characters. A **character** χ of a finite Abelian group is a group homomorphism from G to the multiplicative group $\mathbb{C}^*$ of $\mathbb{C}$. The elements $\chi(g)$ belong to the unit circle of $\mathbb{C}$.

The set of all such characters of a given Abelian group G, when equipped with the point-wise multiplication of mappings, is itself a group (called the **dual group**, denoted by $\widehat{G}$), isomorphic to G. The character $\chi_0 : g \in G \mapsto 1$ is called the **principal** character of G. The characters of a direct product $K \times N$ are given by $\chi = \chi_K \otimes \chi_N$ where $(a, b) \in K \times N$ is mapped to $\chi_K(a)\chi_N(b) \in \mathbb{C}$, and where χ_K is a character of K and χ_N a character of N. The characters of G can be naturally extended by linearity to homomorphisms of algebras from $\mathbb{C}[G]$ to $\mathbb{C}$: if $D = \sum_{g \in G} d_g g \in \mathbb{C}[G]$ and χ is a character of G, then

$$\chi(D) = \sum_{g \in G} d_g \chi(g) \ . \tag{13}$$

There is an important formula for characters of Abelian groups which also holds for non-Abelian groups, see Theorem 9.

Theorem 3 (Inversion formula) *Let G be an Abelian group, and let $D = \sum_{g \in G} d_g g$ be an element in $\mathbb{C}[G]$. Then*

$$d_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(D) \cdot \chi(g^{-1}).$$

Corollary 4 (Parseval's equation) *Let G be an Abelian group. For $D = \sum_{g \in G} d_g g$ in $\mathbb{C}[G]$, we have*

$$\sum_{g \in G} d_g^2 = \frac{1}{|G|} \sum_{\chi \in \hat{G}} |\chi(D)|^2.$$

Proof. This follows easily from the inversion formula applied to the coefficient of the identity element in $D \cdot D^{-1}$. □

Using these characters we can introduce another criterion of nonlinearity: a function $f : K \to N$ (where K and N are both finite and Abelian) is called **maximum nonlinear** if and only if

$$\max_{\chi_N \neq \chi_0} |\chi(D_f)| \leq \max_{\chi_N \neq \chi_0} |\chi(D_g)| \quad \forall g : K \to N \tag{14}$$

or, equivalently

$$\max_{\chi_N \neq \chi_0} |\chi(D_f)| = \min_{g:K\to N} \max_{\chi_N \neq \chi_0} |\chi(D_g)| \ . \tag{15}$$

The value $\sqrt{|K|}$ is a lower bound for the quantity $\max_{\chi_N \neq \chi_0} |\chi(D_f)|$ which follows easily from Parseval's relation for Abelian groups (Corollary 4). A function that reaches this theoretically best bound is called **bent**. A function is bent if and only if it is perfect nonlinear as defined above.. This follows easily by applying characters to the group ring equation (12), see also [10, 21].

Finally, characters allow us to give another characterization for APN functions:

Theorem 5. *Let K and N be two finite Abelian groups. A function $f : K \to N$ is almost perfect nonlinear if and only if*

$$\sum_{\chi} |\chi(D_f)|^4 \leq \sum_{\chi} |\chi(D_g)|^4 \ \forall g : K \to N \ . \tag{16}$$

Proof. (*sketch*) As before, let $G = K \times N$. Consider the coefficient of the identity element in $(D_g D_g^{(-1)})^2$: this is precisely $\sum_{(a,b)\in G} \delta_g(a,b)^2$.. Therefore, minimizing $\sum_{(a,b)\in G} \delta_g(a,b)^2$ is equivalent to minimizing $\sum_{\chi} |\chi(D_g)|^4$. □

Remark 6. *(1) If all character values $\chi(D_f)$ with $\chi_N \neq \chi_0$ are the same, then an almost perfect nonlinear function is actually perfect nonlinear.*

(2) Theorem 5 is well known for the elementary Abelian case (see [11]) and also known for the Abelian case [21]. It is one of the purposes of this paper to show that one can even extend it to the non-Abelian case.

In some particular cases, we know a lower bound for the sum of the fourth-power of the absolute value of $\chi(D_f)$. Indeed when K and N are two elementary Abelian 2-groups of order m, then it can be shown that for each $f : K \to N$,

$$2m^3(m-1) \leq \sum_{\chi \neq \chi_0} |\chi(D_f)|^4 \tag{17}$$

and since $\chi_0(D_f) = |D_f| = |K| = m$, we have

$$m^3(3m-2) \leq \sum_{\chi} |\chi(D_f)|^4 \ . \tag{18}$$

It is very important to note that these arguments only work in the elementary Abelian case: the proofs rely on the fact that the $\delta_f(a,b)$ are always even in characteristic 2. We refer the reader to the original paper [11], see also [10, 21]. Together

with Corollary 4, inequality (17) yields yet another lower bound for the quantity $\max_{\chi_N \neq \chi_0} |\chi(D_f)|$ in the elementary Abelian case:

Theorem 7 ([11]) *Let $f : K \to N$ where K and N are elementary Abelian 2-groups of order $m = 2^n$. Then*

$$\max_{\chi_N \neq \chi_0} |\chi(D_f)| \geq \sqrt{2m} \ . \tag{19}$$

Moreover when n is odd, a function $f : K \to N$ is maximal nonlinear if and only if

$$\max_{\chi_N \neq \chi_0} |\chi(D_f)| = \sqrt{2m} \ . \tag{20}$$

In this case, the function is almost perfect nonlinear and the lower bound given in inequality (18) is reached.

Contrary to the odd case, when n is even obviously the previous lower bound cannot be reached. The lowest possible value of $\max_{\chi_N \neq \chi_0} |\chi(D_f)|$ satisfies (see, for instance [9])

$$\sqrt{2m} < \min_{f:K\to N} \max_{\chi_N \neq \chi_0} |\chi(D_f)| \leq 2\sqrt{m} \ . \tag{21}$$

Moreover, the lowest known value corresponds to the upper bound.

Example 8. *(1) The classical example of an almost perfect nonlinear function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is $f(x) = x^3$, where the group is identified with the additive group of the finite field $\mathbb{F}_{2^n}$. This function is also maximum nonlinear if n is odd. In the n even case, it is a function where the largest nontrivial character value is $2^{\frac{n+2}{2}}$, hence the upper bound in (21) is reached, see [9], for instance.*

(2) Similarly, the classical example of a perfect nonlinear mapping is x^2 defined on $\mathbb{F}_{p^n}$, p odd (this is folklore).

We note that recently many new perfect and almost perfect nonlinear functions have been discovered. It seems that the ideas to construct perfect and almost perfect nonlinear functions are somewhat similar, therefore the discovery of new almost perfect nonlinear functions did influence the investigation of perfect nonlinear functions which are of great interest in finite geometry. For the characteristic 2 case, we refer to [9] and the references cited there, in particular [4, 5, 6, 13, 14]; for the perfect nonlinear case see [1, 7, 8, 23], for instance.

The purpose of this paper is to develop these ideas - almost perfect nonlinearity and maximum nonlinear functions - in a larger context than the classical elementary Abelian 2-groups, namely the case of finite non-Abelian groups. For this objective we introduce the appropriate notion of "non-Abelian characters" in the following section.

2. Basics on group representations

The reader may find the definitions and results listed below (and lot more) in the book [22].

A **(linear) representation** of a finite group G is a pair (ρ, V) where V is a finite-dimensional $\mathbb{C}$-vector space and ρ is a group homomorphism from G to the linear group $GL(V)$. In practice the group homomorphism ρ is often identified with the representation (ρ, V) and we may sometimes use the notation V_ρ to refer to the second component of (ρ, V). The **dimension** of the representation (ρ, V) is defined as the dimension of the vector space V over the complex field and denoted by $\dim \rho$. Two representations (ρ_1, V_1) and (ρ_2, V_2) of the same group G are said to be **equivalent** if there exists a vector space isomorphism $T : V_1 \to V_2$ such that for each $g \in G$,

$$T \circ \rho_1(g) = \rho_2(g) \circ T \ . \tag{22}$$

Two equivalent representations may be identified without danger. Continuing with definitions, a representation (ρ, V) is **irreducible** if the only subvector spaces W of V so that $(\rho(g))(W) \subseteq W$ for every $g \in G$ are the null-space and V itself. The **dual** $\widehat{G}$ of a finite group G is the set of all equivalence classes of irreducible representations of G. When G is an Abelian group, $\widehat{G}$ is dual group of G, as introduced earlier. In particular a finite group is Abelian if and only if all its irreducible representations are one-dimensional. Let $[G, G]$ be the derived subgroup of G, *i.e.*, the subgroup generated by the elements of the form $ghg^{-1}h^{-1}$ for $(g, h) \in G^2$. It is a normal subgroup and the quotient-group $G/[G, G]$ is Abelian. One-dimensional representations of G are related to this derived group since their total number is equal to the order of $G/[G, G]$. The cardinality $|\widehat{G}|$ of the dual of G is equal to the number of conjugacy classes of G. The (equivalence class of the) representation $(\rho_0, \mathbb{C})$ that maps each element of G to the identity map of $\mathbb{C}$ is called the **principal** representation of G. For practical purpose we identify the value $\rho_0(g)$ as the number 1 rather than the identity mapping of $\mathbb{C}$ or, in other terms, we identify $\rho_0(g)$ and its trace $tr(\rho_0(g)) = 1$.

We can also construct some linear representations from existing ones. For instance, given the dual sets of two finite groups K and N, one can build up the dual $\widehat{K \times N}$ of their direct product. This construction uses the notion of tensor product of two vector spaces. So let V_1 and V_2 be two complex vector spaces. We call **tensor product** of V_1 and V_2 a vector space W equipped with a bilinear mapping $j : V_1 \times V_2 \to W$ such that the following property holds. For each $\mathbb{C}$-vector space V_3 and for each bilinear mapping $f : V_1 \times V_2 \to V_3$ there exists one and only one linear mapping $\tilde{f} : W \to V_3$ such that $\tilde{f} \circ j = f$. It can be shown that there is one and only one such vector space W (up to isomorphism). It is denoted by $V_1 \otimes V_2$. Moreover if $(e_k^{(1)})_k$ is a basis of V_1 and $(e_\ell^{(2)})_\ell$ is a basis of V_2, then the family $(j(e_k^{(1)}, e_\ell^{(2)}))_{(k,\ell)}$ is a basis of W. This property shows that

$$\dim(V_1 \otimes V_2) = \dim(V_1) \dim(V_2) \ . \tag{23}$$

In particular for every vector space V, we have $V \otimes \mathbb{C} = \mathbb{C} \otimes V = V$ (equality up to isomorphism). For $(v_1, v_2) \in V_1 \times V_2$, we denote $j(v_1, v_2)$ by $v_1 \otimes v_2$. Since j (and therefore $\otimes$) is a bilinear mapping we have $(\alpha v_1 + \beta w_1) \otimes v_2 = \alpha v_1 \otimes v_2 + \beta w_1 \otimes v_2$ and the corresponding equality holds for the second variable. So now let $\rho_1 : K \to GL(V_1)$ and $\rho_2 : N \to GL(V_2)$ be two representations. Then we define a representation $\rho_1 \otimes \rho_2$ of $K \times N$ in $V_1 \otimes V_2$ by

$$(\rho_1 \otimes \rho_2)(k, n) = \rho_1(k) \otimes \rho_2(n) \quad \text{with } (k, n) \in K \times N \ . \tag{24}$$

Moreover, one can show that if ρ_1 and ρ_2 are both irreducible then $\rho_1 \otimes \rho_2$ is an irreducible representation of $K \times N$. And reciprocally, every irreducible representation of $K \times N$ is equivalent to a representation of the form $\rho_1 \otimes \rho_2$, where ρ_1 (resp. ρ_2) is an irreducible representation of K (resp. N). Given an irreducible representation ρ of $K \times N$, we use ρ_K and ρ_N to denote the representations of K and N such that ρ is equivalent to $\rho_K \otimes \rho_N$. A system of representatives of equivalence classes of irreducible representations of $K \times N$ is given by this way. Actually, the classes of representations of a given group G may be used to form a ring: just take the free Abelian group generated by all isomorphism classes of representations of G, mod out by the subgroup generated by elements of the form $\rho_1 + \rho_2 - (\rho_1 \oplus \rho_2)$, where $\rho_1 \oplus \rho_2$ is the obvious direct sum of two (classes of) representations. It can be proved that the irreducible representations form a basis for this $\mathbb{Z}$-module. The ring structure, called the **representation ring of** G, is then given simply by tensor product $\rho_1 \otimes \rho_2 : g \in G \mapsto \rho_1(g) \otimes \rho_2(g) \in GL(V_1 \otimes V_2)$, defined on these generators and extended by linearity.

Note that every irreducible representation is equivalent to a unitary representation *i.e.* a representation ρ such that $\rho(g^{-1}) = \rho(g)^*$, where the star denotes the usual adjoint operation. Indeed, let $\rho : G \to GL(V)$ be a representation of a finite group G, where V is an Hermitian space (together with a scalar product $\langle \cdot, \cdot \rangle$) and let us consider the following Hermitian product: $\langle x, y \rangle_\rho = \sum_{g \in G} \langle \rho(g)(x), \rho(g)(y) \rangle$. It is easy to prove that for every $x, y \in V$ and every $g \in G$, $\langle \rho(g)(x), \rho(g)(y) \rangle_\rho = \langle x, y \rangle_\rho$ in such a way that $\rho(g)$ is unitary with respect to $\langle \cdot, \cdot \rangle_\rho$ for each $g \in G$. Therefore, in what follows we assume that $\widehat{G}$ is actually a complete set of representatives of non-isomorphic irreducible representations, all of them being unitary.

We naturally extend a representation (ρ, V) by linearity to an algebra homomorphism from $\mathbb{C}[G]$ to $End(V)$, the linear endomorphisms of V, by

$$\rho(D) = \sum_{g \in G} d_g \rho(g) \ , \tag{25}$$

with $D = \sum_{g \in G} d_g g$. As a particular case one can prove the following relations:

$$\rho(G) = \begin{cases} 0_V \text{ if } \rho \neq \rho_0 \ , \\ |G| \text{ if } \rho = \rho_0 \end{cases} \tag{26}$$

for every $\rho \in \widehat{G}$, and

$$\sum_{\rho\in\widehat{G}} \dim\rho \ tr(\rho(g)) = \begin{cases} |G| \text{ if } g = 1_G \ , \\ 0 \ \text{ if } g \neq 1_G \ . \end{cases} \tag{27}$$

For $D \in \mathbb{C}[G]$ we may define its *Fourier transform* as $\widehat{D} = \sum_{\rho\in\widehat{G}} \rho(D)\rho$, which can be identified with $(\rho(D))_{\rho\in\widehat{G}} \in \bigoplus_{\rho\in\widehat{G}} End(V_\rho)$. Then the Fourier transform is the mapping

$$\begin{array}{rcl} \mathcal{F} : \mathbb{C}[G] & \to & \bigoplus_{\rho\in\widehat{G}} End(V_\rho) \\ D & \mapsto & \widehat{D} \ . \end{array} \tag{28}$$

Note that in the case where G is a finite Abelian group, then every irreducible representation is one-dimensional and $End(\mathbb{C})$ is isomorphic to $\mathbb{C}$. Therefore for $D \in \mathbb{C}[G]$, we have $\widehat{D} \in \bigoplus_{\rho\in\widehat{G}} \mathbb{C} \simeq \mathbb{C}[\widehat{G}]$.

The coefficients $\rho(D)$ of the Fourier transform $\widehat{D}$ of D are used in the sequel to study nonlinear properties of functions $f : K \to N$ in the general case where both K and N are finite groups, not necessarily commutative.

3. Almost perfect nonlinearity

In this section, we develop a Fourier characterization of APN functions in the non-Abelian setting, using group representations. We also introduce the relevant notion of bentness in this context and we show that, contrary to the classical case, this is not equivalent to perfect nonlinearity in this general framework.

Let G be a finite group. The following theorem is well known; we include a proof to keep the paper more self-contained.

Theorem 9 (Fourier inversion, Parseval's equation) *Let $D = \sum_{g\in G} d_g g$ be an element in the group algebra $\mathbb{C}[G]$. Then the following holds:*

$$d_g = \frac{1}{|G|} \sum_{\rho\in\widehat{G}} \dim\rho \ tr(\rho(D) \circ \rho(g^{-1})) \quad (\textit{Fourier inversion}) \tag{29}$$

$$\sum_{g\in G} |d_g|^2 = \frac{1}{|G|} \sum_{\rho\in\widehat{G}} \dim\rho \ \|\rho(D)\|^2 \quad (\textit{Parseval's equation}) \tag{30}$$

where $\|f\|$ is the ***trace norm*** *of a linear endomorphism f given by $\|f\| = \sqrt{tr(f \circ f^*)}$.*

Proof. We have

$$\begin{aligned}
&\sum_{\rho\in\widehat{G}} \dim\rho \ tr(\rho(D)\circ\rho(g^{-1})) \\
&= \sum_{\rho\in\widehat{G}} tr\left(\rho(\sum_{h\in G} d_h h)\circ\rho(g^{-1})\right) \\
&= \sum_{h\in G} d_h \sum_{\rho\in\widehat{G}} \dim\rho \ tr(\rho(hg^{-1})) \text{ (by linearity of the trace and } \rho) \\
&= |G| d_g \text{ (according to eq. (27))}.
\end{aligned} \tag{31}$$

This proves the Fourier inversion formula.

We have

$$DD^{(-1)} = \sum_{g\in G}\left(\sum_{h\in G} d_h \overline{d_{g^{-1}h}}\right) g \ . \tag{32}$$

In particular the coefficient of the identity 1_G in this formal sum is $\sum_{g\in G} |d_g|^2$. We can also compute this coefficient by using the Fourier inversion on $DD^{(-1)}$. It is given by

$$\begin{aligned}
&\frac{1}{|G|}\sum_{\rho\in\widehat{G}} \dim\rho \ tr(\rho(DD^{(-1)})) \\
&= \frac{1}{|G|}\sum_{\rho\in\widehat{G}} \dim\rho \ tr(\rho(D)\circ\rho(D)^*)) \text{ (since } \rho \text{ is unitary)} \\
&= \frac{1}{|G|}\sum_{\rho\in\widehat{G}} \dim\rho \|\rho(D)\|^2 \ .
\end{aligned} \tag{33}$$

We may assume that $\widehat{G}$ is a set of unitary representatives of irreducible representations. Therefore Parseval's equation holds. □

Using group representations we obtain an alternative formulation for almost perfect nonlinearity. Note that the definition of almost perfect nonlinearity given in eq. (2) holds for the Abelian as well as non-Abelian situation.

Theorem 10. *Let K and N be two finite groups. Let G be the direct product $K\times N$. A function $f : K \to N$ is almost perfect nonlinear if and only if*

$$\sum_{\rho\in\widehat{G}} \dim\rho \ \|\rho(D_f)\|^4 \leq \sum_{\rho\in\widehat{G}} \dim\rho \ \|\rho(D_g)\|^4, \ \forall g : K \to N \ . \tag{34}$$

Proof. We have $D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b)$. So using Parseval's equation we

obtain:

$$\begin{aligned}\sum_{(a,b)\in G}\delta_f(a,b)^2 &= \frac{1}{|G|}\sum_{\rho\in\widehat{G}}\dim\rho\ \|\rho(D_f D_f^{(-1)})\|^2\\ &= \frac{1}{|G|}\sum_{\rho\in\widehat{G}}\dim\rho\ \|\rho(D_f)\circ\rho(D_f)^*\|^2\\ &= \frac{1}{|G|}\sum_{\rho\in\widehat{G}}\dim\rho\ \|\rho(D_f)\|^4\ .\end{aligned} \tag{35}$$

Because a function $f : K \to N$ is APN if and only if for every $g : K \to N$,

$$\sum_{(a,b)\in G}\delta_f(a,b)^2 \leq \sum_{(a,b)\in G}\delta_g(a,b)^2, \tag{36}$$

this concludes the proof. □

Group representations can be used to find another criterion for the nonlinearity of functions. As before, K and N are both finite groups of order m and n, and $f : K \to N$. For some $\rho \in \widehat{K \times N}$, the values of $\rho(D_f)$ are known:

$$\rho(D_f) = \begin{cases} m \ \text{ if } \rho = \rho_0\ , \\ 0_V \text{ if } \rho = \rho_K \otimes \rho_0 \text{ and } (\rho_K, V) \text{ is nonprincipal on } K\ . \end{cases} \tag{37}$$

Indeed first let us suppose that ρ is principal on G. Then we have

$$\begin{aligned}\rho_0(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_0(a,b)\\ &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\\ &= |D_f|\\ &= |K|\\ &= m\ .\end{aligned} \tag{38}$$

Now let us suppose that $\rho = \rho_K \otimes \rho_0$ with (ρ_K, V) nonprincipal on K. Then we have

$$\begin{aligned}\rho(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_K(a)\otimes\rho_0(b)\\ &= \sum_{a\in K}\rho_K(a)\otimes\rho_0(f(a))\\ &= \sum_{a\in K}\rho_K(a)\ (\text{since } V\otimes\mathbb{C} = V)\\ &= \rho_K(K)\\ &= 0_V\ (\text{according to eq. (26)})..\end{aligned} \tag{39}$$

Parseval's equation and an analogy with the Abelian case, suggest us to say that a function $f : K \to N$ is called **maximum nonlinear** if and only if the value

$\sqrt{\dim \rho}\|\rho(D_f)\|$ is as small as possible, or in other terms (using the known values of $\rho(D_f)$)

$$\max_{\rho_N \neq \rho_0} \sqrt{\dim \rho}\ \|\rho(D_f)\| \leq \max_{\rho_N \neq \rho_0} \sqrt{\dim \rho}\ \|\rho(D_g)\|\ \forall g : K \to N\ . \tag{40}$$

As in the Abelian case, we obtain the following lower bound for this quantity:

Theorem 11. *Let $f : K \to N$. Then*

$$\max_{\rho_N \neq \rho_0} \dim \rho\ \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\widehat{K}|(|\widehat{N}|-1)}\ . \tag{41}$$

Proof. By Parseval's equation applied to D_f, we have

$$\begin{aligned} \frac{1}{|G|}\sum_{\rho \in \widehat{G}} \dim \rho\ \|\rho(D_f)\|^2 &= \sum_{(a,b)\in G} 1_{D_f}(a,b)^2 \\ &= m\ . \end{aligned} \tag{42}$$

So we have

$$\sum_{\rho \in \widehat{G}} \dim \rho\ \|\rho(D_f)\|^2 = |G|m = m^2 n\ . \tag{43}$$

We know some values of $\rho(D_f)$ that allow us to compute the following sum:

$$\begin{aligned} \sum_{\rho_N \neq \rho_0} \dim \rho\ \|\rho(D_f)\|^2 &= \sum_{\rho \in \widehat{G}} \dim \rho\ \|\rho(D_f)\|^2 - \sum_{\rho_N = \rho_0} \dim \rho\ \|\rho(D_f)\|^2 \\ &= m^2 n - \underbrace{\dim \rho_0\ \|\rho_0(D_f)\|^2}_{=m^2} - \underbrace{\sum_{\rho_N = \rho_0,\ \rho \neq \rho_0} \dim \rho\ \|\rho(D_f)\|^2}_{=0} \\ &\quad \text{(according to eq. (43) and eq. (37))} \\ &= m^2(n-1)\ . \end{aligned} \tag{44}$$

Now we need to evaluate the number of principal representations on N: it is equal to $|\widehat{K}|$. Then there are $|\widehat{G}| - |\widehat{K}|$ nonprincipal representations on N. But $|\widehat{G}| = |\widehat{K}||\widehat{N}|$. Therefore we have

$$\max_{\rho_N \neq \rho_0} \dim \rho\ \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\widehat{K}|(|\widehat{N}|-1)}\ . \tag{45}$$

□

The proof also shows that

$$\max_{\rho_N \neq \rho_0} \dim \rho\ \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{|\widehat{K}|(|\widehat{N}|-1)} \quad \Leftrightarrow \quad \forall \rho_N \neq \rho_0,\ \|\rho(D_f)\|^2 = \Gamma, \tag{46}$$

where

$$\Gamma = \frac{m^2(n-1)}{\dim \rho |\widehat{K}|(|\widehat{N}|-1)}\ .$$

In the Abelian case, the righthand side of this equivalence turns out to be the definition of bent functions since $\dim \rho = 1$, $|\widehat{K}| = m$ and $|\widehat{N}| = n$. It is well known that classical bentness is equivalent to perfect nonlinearity, as we stated before. Now if we take the righthand side of equivalence (46) as a natural definition for **bentness** in the non-Abelian case, we can prove this notion to be nonequivalent to perfect nonlinearity in many situations. Let us suppose that $f : K \to N$ is both perfect nonlinear and bent. Since f is perfect nonlinear its graph D_f, as an element of $\mathbb{Z}[G]$, satisfies the famous group ring equation (12) for relative $(m, n, m, \frac{m}{n})$. difference sets So for $(\rho, V) \in \widehat{G}$, we have

$$\rho(D_f D_f^{(-1)}) = mId_V + \lambda(\rho(G) - \rho(N)) \ , \tag{47}$$

where Id_V denotes the identity mapping of V. Now let us suppose that $\rho_N \neq \rho_0$. So we have $\rho(G) = 0_V$ and $\rho(N) = \rho_K(1_K) \otimes \rho_N(N) = 0_V$ according to eq. (26). Then in this case we obtain:

$$\rho(D_f D_f^{(-1)}) = \rho(D_f) \circ \rho(D_f)^* = mId_V \ . \tag{48}$$

By using the trace on both sides of the last equality above, we have for $\rho_N \neq \rho_0$

$$\|\rho(D_f)\|^2 = m \dim \rho. \tag{49}$$

But since f is bent, combining eq. (49) and the righthand side of equivalence (46),

$$m(n-1) = (\dim \rho)^2 |\widehat{K}|(|\widehat{N}| - 1) \ . \tag{50}$$

This equality may hold if and only if $\dim \rho$ is the same for every $\rho \in \widehat{G}$ such that $\rho_N \neq \rho_0$ (we exclude the trivial case where $|N| = 1$); this is for instance the case if both K and N are Abelian. We can show that in the case where at least one of K or N is non-Abelian and distinct of its derived group[a] (for instance it is a non sovable group), and N, when Abelian, is not reduced to the trivial group, then the previous equality cannot hold and therefore perfect nonlinearity and bentness - as introduced by analogy - are nonequivalent and even paradoxical in this non-Abelian setting:

1. First let us suppose that N is a non-Abelian group such that $N \neq [N, N]$ (this is the case of non solvable groups). By assumption N has at least one irreducible representation of dimension $d > 1$ (it is *ipso facto* a nonprincipal representation), call it $\rho_N^{(1)}$. Since the number of one-dimensional representations of N is exactly $|N/[N, N]|$, there is also at least one such representation which is nonprincipal (for if $|N/[N, N]| = 1$ then $N = [N, N]$). Call $\rho_N^{(2)}$ one of them.. Now let ρ_K be any d'-dimensional irreducible representation of K, then $\rho_K \otimes \rho_N^{(i)}$ (for $i = 1, 2$) are both irreducible nonequivalent representations of $G = K \times N$ which are non principal on N. We have $\dim \rho_K \otimes \rho_N^{(1)} = d'd > \dim \rho_K \otimes \rho_N^{(2)} = d'$.

[a]If for a nonabelian group H, $H \neq [H, H]$ then H is not a simple group.

2. Secondly, let us suppose that K is a non-Abelian group such that $K \neq [K, K]$ and, if N is non-Abelian then $N \neq [N, N]$ and if N is Abelian then it is not reduced to the trivial group, *i.e.*, $|N| > 1$. According to case 1., we already know that K has at least one nonprincipal one-dimensional representation, call it $\rho_K^{(1)}$, and at least one irreducible representation of dimension $d > 1$, call it $\rho_K^{(2)}$. If N is Abelian, since it is not the trivial group, it has at least one nonprincipal (one-dimensional) representation. According to 1., this is also the case if N is non-Abelian and $N \neq [N, N]$; call ρ_N this representation. Then $\rho_K^{(i)} \otimes \rho_N$ (for $i = 1, 2$) are both irreducible nonequivalent representations of $G = K \times N$ which are nonprincipal on N. We have $\dim \rho_K^{(1)} \otimes \rho_N = 1 < \dim \rho_K^{(2)} \otimes \rho_N = d$.

4. Some computational results and open questions

In this section we present some results given by formal computations using GAP [15] and MAGMA [3]. There are three goals:

- *Almost perfect nonlinearity*, see Theorem 10: Minimize
$$\sum_{\rho \in \widehat{G}} \dim \rho \; \|\rho(D_f)\|^4$$
for functions $f : K \to N$, where $G = K \times N$.
- *Maximal nonlinearity*, see eq. (40): Minimize the maximum of
$$\sqrt{\dim \rho} \; \|\rho(D_f)\|$$
for all $f : K \to N$.
- *Bentness*, see eq. (46): Find functions $f : K \to N$ such that
$$\forall \rho_N \neq \rho_0, \; \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{\dim \rho |\widehat{K}|(|\widehat{N}| - 1)}.$$

We note that besides the bounds given in this paper, no general results for arbitrary groups are known. Here we do not want to give extensive computational results but we want to indicate some interesting phenomena which occur in the non-Abelian setting. Note that for groups K and N, we have to go through **all** mappings $K \to N$, whose number is $|N|^{|K|}$. Hence the approach to find "good" functions by a complete search is very limited, and it would be interesting to find theoretical constructions which are **provable** maximal nonlinear or almost perfect nonlinear.

Let us begin with the two goups of order 6, the cyclic group $\mathbb{Z}_6$ and the symmetric group $\mathcal{S}_3$. In Table 1, we list the "best" values (marked in boldface) both for the maximum nonlinearity as well as almost perfect nonlinearity.

It is remarkable that the measure of almost perfect nonlinearity is by far the least in the case $(K, N) = (\mathcal{S}_3, \mathbb{Z}_6)$ and not in the Abelian case. Moreover, if $(K, N) = (\mathcal{S}_3, \mathbb{Z}_6)$ each almost perfect nonlinear functions is also maximal nonlinear. This situation fails to be true in all the other cases where no almost perfect nonlinear function is also maximal nonlinear.

Table 1. Non-Abelian groups K, N of order 6, $f : K \to N$

K	N	$\min_{g:K\to N} \sum_{\rho\in\widehat{G}} \dim\ \rho \|\rho(D_g)\|^4$	$\min_{g:K\to N} \max_{\rho\|_N\neq\rho_0} \sqrt{\dim\ \rho}\|\rho(D_g)\|$
$\mathcal{S}_3$	$\mathbb{Z}_6$	**2376**	4
$\mathbb{Z}_6$	$\mathcal{S}_3$	3972	$4\sqrt{2}$
$\mathcal{S}_3$	$\mathcal{S}_3$	3552	$2\sqrt{14}$
$\mathbb{Z}_6$	$\mathbb{Z}_6$	2808	$\mathbf{2\sqrt{3}}$

We also made a complete search for the case of abelian groups of order 8 (Table 2).

Table 2. Abelian groups K, N of order 8, $f : K \to N$

K	N	$\min_{g:K\to N} \sum_{\rho\in\widehat{G}} \|\rho(D_g)\|^4$	$\min_{g:K\to N} \max_{\rho\|_N\neq\rho_0} \|\rho(D_g)\|$
$\mathbb{Z}_8$	$\mathbb{Z}_8$	8832	$\sqrt{10+4\sqrt{2}}$
$\mathbb{Z}_8$	$\mathbb{Z}_4\times\mathbb{Z}_2$	8576	4
$\mathbb{Z}_8$	$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	9216	4
$\mathbb{Z}_4\times\mathbb{Z}_2$	$\mathbb{Z}_8$	8960	4
$\mathbb{Z}_4\times\mathbb{Z}_2$	$\mathbb{Z}_4\times\mathbb{Z}_2$	9216	4
$\mathbb{Z}_4\times\mathbb{Z}_2$	$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	10240	4
$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\mathbb{Z}_8$	9216	4
$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\mathbb{Z}_4\times\mathbb{Z}_2$	10240	4
$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	11264	4

The case $K = N = \mathbb{Z}_8$ is of interest: Here the maximum character value is strictly smaller than 4, hence there is a function which is "better" than in the elementary-Abelian case[b]. In contrast to the other cases, this "smallest" maximum is not reached for the functions which minimize the sum of the fourth powers of the character values (which is 8960).

We also searched for bent functions from $\mathcal{S}_3$ to a group N such that $1 < |N| \leq 5$. Note that, in contrast to the Abelian case, the existence question for bent functions $K \to N$ is also meaningful if $|N|$ is not a divisor of $|K|$. The results that we obtained are as follows: First of all, there is no bent functions if $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$. But there is (at least) one bent function $f : \mathcal{S}_3 \to \mathbb{Z}_3$. Indeed we can check that the map f defined by $f(id) = f((1,2)) = f((2,3)) = f((1,3)) = 0$ and $f((1,2,3)) = f((1,3,2)) = 1$ is bent, that is to say that $\sqrt{\dim\rho}\|\rho(D_f)\| = 2\sqrt{3}$ for all $\rho|\mathbb{Z}_3 \neq \rho_0$. The group $\mathcal{S}_3$ has two one-dimensional representations and one two-dimensional representation, and $\mathbb{Z}_3$ has three one-dimensional representations therefore $\frac{|\mathcal{S}_3|^2(|\mathbb{Z}_3|-1)}{|\widehat{\mathcal{S}_3}|(\widehat{\mathbb{Z}_3}-1)|} = 12$. We have $\sqrt{\dim\rho}\|\rho(D_f)\| = 2\sqrt{3}$ for each representation

[b]An example of the graph of such a function is $\{(0,0),(1,5),(2,7),(3,7),(4,7),(5,4),(6,5),(7,4)\}$

$\rho \in \widehat{\mathcal{S}_3 \times \mathbb{Z}_3}$ which is nonprincipal on $\mathbb{Z}_3$. Due to the fact that $\mathcal{S}_3$ has a representation of dimension greater than 1, f is not perfect nonlinear (see the discussion at the end of the previous section).

Finally, we would like to raise some questions. Regarding these questions, both computational results as well as infinite families are, of course, welcome.

(1) Regarding the caracterisation of APN functions by mean of the sum $\sum_{\rho \in \widehat{G}} \dim \rho \, \|\rho(D_f)\|^4$ given in Theorem 10, it should be interesting to find some functions $f : K \to N$ for which this sum reaches some value which is better than the one in the classical case of elementary Abelian groups.
(2) Find functions $f : K \to N$ such that $\dim \rho \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{|\widehat{K}|(|\widehat{N}|-1)}$ for all ρ nonprincipal on N *i.e.* non-Abelian bent functions).
(3) Find functions $f : K \to N$ with $|K| = |N| = 2^n = m$ (n even so that there are no almost bent functions) such that $\max_{\rho_N \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 < 4m$, that is to say functions which are better than the known maximum nonlinear functions in the elementary-Abelian case.
(4) Find functions $f : K \to N$ with $|K| = |N| = 2^n = m$ (n odd, so that there are almost bent functions) such that $\max_{\rho_N \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 < 2m$, that is to say functions which are better than classical almost bent functions. Note that we found such an example for a mapping $f : \mathbb{Z}_8 \to \mathbb{Z}_8$.

References

[1] J. Bierbrauer, New semifields, PN and APN functions, Des. Codes Cryptography, 54 (2010), pp. 189–200.
[2] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptology, 4 (1991), pp. 3–72.
[3] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. the user language, J. Symbolic Comput., 24 (1997), pp. 235–265.
[4] C. Bracken, E. Byrne, N. Markin, and G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, Finite Fields Appl., 14 (2008), pp. 703–714.
[5] L. Budaghyan and C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Trans. Inf. Th., 54 (2008), pp. 2354–2357.
[6] L. Budaghyan, C. Carlet, and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, IEEE Trans. Inf. Th., 54 (2008), pp. 4218–4229.
[7] L. Budaghyan and T. Helleseth, New commutative semifields defined by new PN multinomials. to appear in: Cryptography and Communications.
[8] L. Budaghyan and T. Helleseth, New perfect nonlinear multinomials over $F_{p^{2k}}$ for any odd prime p, in SETA '08: Proceedings of the 5th international conference on Sequences and Their Applications, Berlin, Heidelberg, 2008, Springer-Verlag, pp. 403–414.
[9] C. Carlet, Vectorial boolean functions for cryptography, in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. L.

Hammer, eds., no. 134 in Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2010, ch. 9, pp. 398–471.

[10] C. Carlet and C. Ding, Highly nonlinear mappings, J. Complexity, 20 (2004), pp. 205–244.

[11] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, in Advances in Cryptology – EUROCRYPT 94, A. D. Santis, ed., vol. 950 of Lecture Notes in Computer Science, New York, 1995, Springer-Verlag, pp. 356–365.

[12] J. A. Davis, Construction of relative difference sets in p-groups, Discrete Math., 103 (1992), pp. 7–15.

[13] Y. Edel, G. Kyureghyan, and A. Pott, A new APN function which is not equivalent to a power mapping, IEEE Trans. Inform. Theory, 52 (2006), pp. 744–747.

[14] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Adv. Math. Commun., 3 (2009), pp. 59–81.

[15] S. Linton, Gap: groups, algorithms, programming, ACM Communications in Computer Algebra, 41 (2007), pp. 108–109.

[16] S. L. Ma and B. Schmidt, On (p^a, p, p^a, p^{a-1})-relative difference sets, Des. Codes Cryptogr., 6 (1995), pp. 57–71.

[17] M. Matsui, Linear cryptanalysis method for DES cipher., in Advances in Cryptology – EUROCRYPT 93, T. Helleseth, ed., vol. 765 of Lecture Notes in Computer Science, Springer-Verlag, New York, 1993, pp. 386–397.

[18] K. Nyberg, Perfect nonlinear S-boxes, in Advances in cryptology—EUROCRYPT '91 (Brighton, 1991), Springer, Berlin, 1991, pp. 378–386.

[19] ———, On the construction of highly nonlinear permutations, in Advances in cryptology—EUROCRYPT '92 (Balatonfüred, 1992), vol. 658 of Lecture Notes in Comput. Sci., Springer, Berlin, 1993, pp. 92–98.

[20] A. Pott, A survey on relative difference sets, in Groups, Difference Sets, and the Monster. Proceedings of a Special Research Quarter at the Ohio State University, Spring 1993, K. T. Arasu, J. Dillon, K. Harada, S. Sehgal, and R. Solomon, eds., Berlin, 1996, Walter de Gruyter, pp. 195–232.

[21] ———, Nonlinear functions in abelian groups and relative difference sets, Discrete Appl. Math., 138 (2004), pp. 177–193.

[22] J.-P. Serre, Représentations linéaires des groupes finis, Hermann, Paris, 1967.

[23] Z. Zha, G. M. Kyureghyan, and X. Wang, Perfect nonlinear binomials and their semifields, Finite Fields and Their Applications, 15 (2009), pp. 125 – 133.